



S&H Form: (2/01)

Docket No.: 1083.1048

MT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent No. 6,829,592 B1 :

Takayuki HASEBE et al.

Serial No. 09/000,924

Group Art Unit: 2165

Confirmation No. 5955

Issued: December 7, 2004

Examiner: Nguyen, C.

For: DATA PROTECTION SYSTEM, DATA PREPARATION DEVICE, AND DATA WORKING  
DEVICE

**REQUEST FOR RECONSIDERATION**

Attention: **Decisions and Certificate of Correction Branch**

Commissioner for Patents  
PO Box 1450  
Alexandria, VA 22313-1450

**Certificate**

OCT 25 2007

**of Correction**

In response to the Decision on Request for Certificate of Correction mailed April 27, 2007, the Patentee respectfully requests further consideration of the Request for Certificate of Correction for the above-identified patent filed January 17, 2007, based upon the following accompanying additional support.

The Patentee points to the attached Letter to the Examiner Requesting Consideration and Acknowledgment of Information Disclosure Statement (IDS), including the IDS, filed January 22, 2004 (including USPTO stamped postcard). In the IDS of January 22, 2004, Attachments 1(e) and 1(g) provides that all six (6) of the subject Japanese language references were cited in the English language Japanese Office Action cited in Attachment 1(g). Thus, submission of the subject Japanese references complies with 37 CFR 1.98, because these non-English language publications were cited on the enclosed English language Japanese action which indicates degree of relevance found by the foreign office (MPEP 609).

Patentee encloses another copy of the Letter to the Examiner and the IDS of January 22, 2004 along with the copies of the IDS citations.

Reconsideration of the Request for Certificate of Correction for the above-identified patent filed January 17, 2007, is respectfully requested.

If any further fees are required in connection with this Request for Reconsideration,  
please charge our Deposit Account No. 19-3935.

Respectfully submitted,  
STAAS & HALSEY LLP

Date: October 23, 2007

By: 

Mehdi Sheikerz  
Registration No. 41,307

1201 New York Ave, N.W., 7th Floor  
Washington, D.C. 20005  
Telephone: (202) 434-1500  
Facsimile: (202) 434-1501

MS



Req. for COC filed 1-18-07

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents  
United States Patent and Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450  
www.uspto.gov

1083.1048

Date Mailed : April 27, 2007  
Serial No. : 09/000924  
Patent No. : 6,829,592 B1  
Patent Issued : Dec. 7, 2004  
Inventor(s) : Takayuki Hasebe, et al.  
Title : DATA PROTECTION SYSTEM, DATA PREPARATION DEVICE, AND  
DATA WORKING DEVICE

Re: Request for Certificate of Correction

Consideration has been given your request for the issuance of a certificate of correction for the above-identified patent.

Respecting the alleged errors noted in your request, all references are Japanese and there is no translation attached.

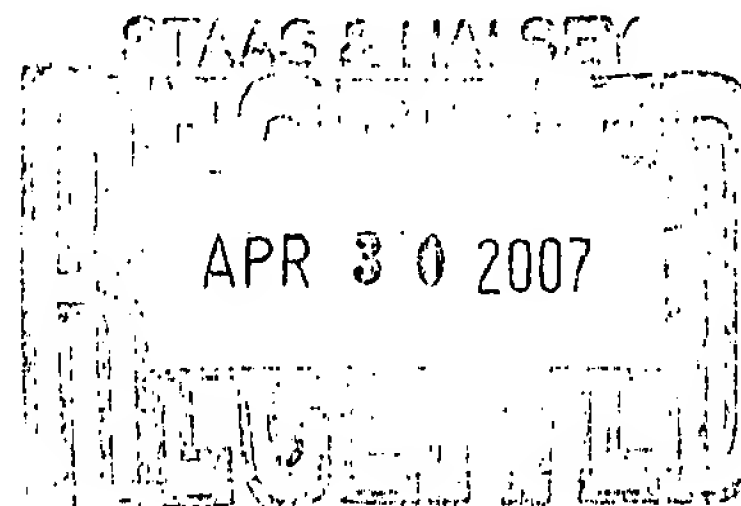
In view of the foregoing your request is hereby denied.

Further consideration will be given upon receipt of a Request for Reconsideration, which should be directed to Decisions and Certificate of Correction Branch. Requests for Reconsideration should be accompanied by additional support (e.g. copy of amendments, post card receipts. PTOL 1449 or 892, etc.), containing requested data or changes) and/or brief statements of facts, as requested.

Magdalene Talley  
For Cecelia B. Newman, Supervisor  
Decisions and Certificate  
Of Correction Branch  
(703) 308-9390 ext. 116  
FAX 571-270-9942

Staas & Halsey LLP  
1201 New York Ave., NW, 7<sup>th</sup> Fl.  
Washington, DC 20005

CBN/mt



Please Date Stamp and return

Information Disclosure Statement with Form PTO-1449, Attachments 1(e) and 1(g), with copy of Japanese Office Action, including copy of English translation thereof, six references; Letter to the Examiner (2 pages) with IDS certification (1 p.); and a check in the amount of \$180.00.

APPLICANT(S): Takayuki HASEBE et al.

SERIAL NO: 09/000,924

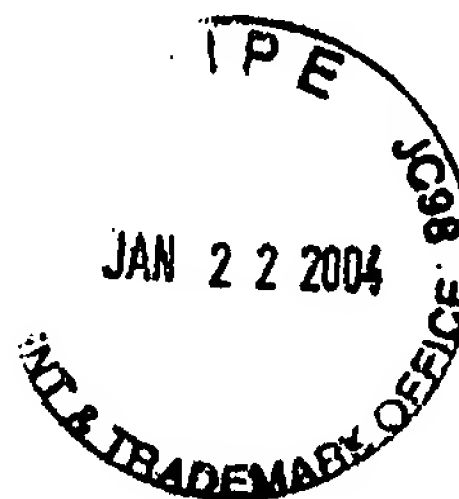
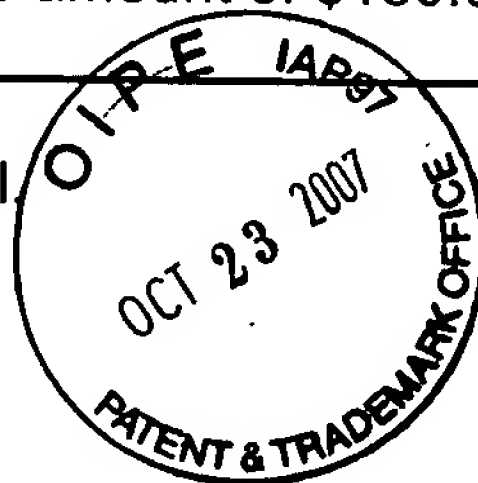
CONFIRMATION NO. 5955

TITLE: DATA PROTECTION SYSTEM, DATA PREPARATION DEVICE, AND DATA WORKING DEVICE

FILING DATE: December 30, 1997

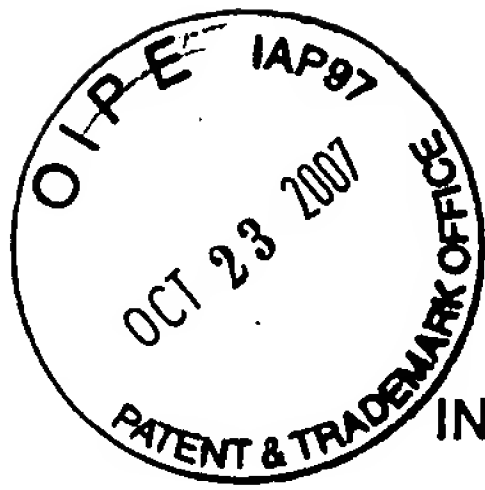
DOCKET NO: 1083.1048/MS:mt

DUE DATE: April 6, 2004



13





Docket No.: 1083.1048

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

Takayuki HASEBE et al..

Group Art Unit: 2165

Serial No. 09/000,924

Filed: December 30, 1997

Examiner: Nguyen, C.

For: DATA PROTECTION SYSTEM, DATA PREPARATION DEVICE, AND DATA WORKING  
DEVICE

LETTER TO THE EXAMINER

REQUESTING CONSIDERATION AND ACKNOWLEDGMENT OF  
INFORMATION DISCLOSURE STATEMENT

**Mail Stop: ISSUE FEE**

Commissioner for Patents  
PO Box 1450  
Alexandria, VA 22313-1450

Sir:

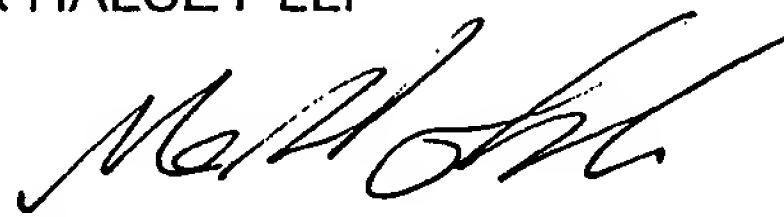
An Information Disclosure Statement (IDS) is submitted herewith and the IDS fee for the same has been paid. The above-identified US application has been allowed. The Issue Fee has not been paid.

It is respectfully requested that the Examiner fully consider and acknowledge the Information Disclosure Statement, including Form PTO 1449 and Attachments 1(e) and 1(g), because the Information Disclosure Statement discloses a Japanese Office Action in a counterpart Japanese Patent Application No. JP 1997-154046 of the above-identified US patent application, and pursuant to 37 CFR 1.97(d) and (e)(1), as asserted in the attached IDS certification, the information contained in the Information Disclosure Statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the Information Disclosure Statement.

If there are any additional fees associated with filing of this communication, please charge the same to our Deposit Account No. 19-3935.

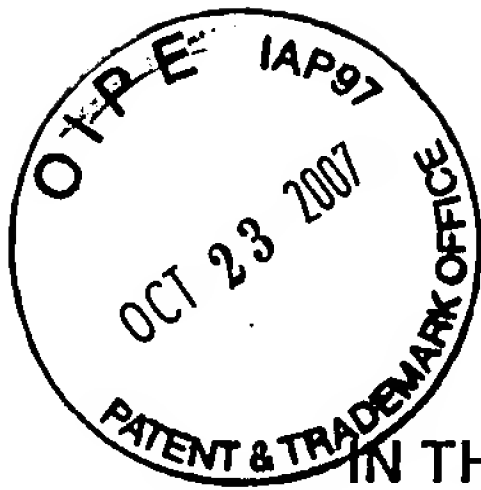
Respectfully submitted,  
STAAS & HALSEY LLP

Date: 1/22/2004

By: 

Mehdi Sheikerz  
Registration No. 41,307

1201 New York Avenue, NW, Suite 700  
Washington, D.C. 20005  
(202) 434-1500



# COPY

Attorney Docket No. 1083.1048

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Takayuki HASEBE et al.

Application No.: 09/000,924

Group Art Unit: 2165

Filed: December 30, 1997

Examiner: Nguyen, C.

For: DATA PROTECTION SYSTEM, DATA PREPARATION DEVICE, AND DATA WORKING DEVICE

## INFORMATION DISCLOSURE STATEMENT

MAIL STOP: ISSUE FEE  
Commissioner for Patents  
PO Box 1450  
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure provisions of 37 CFR § 1.56, there is hereby provided certain information which the Examiner may consider material to the examination of the subject U.S. patent application. It is requested that the Examiner make this information of record if it is deemed material to the examination of the subject application.

1. Enclosures accompanying this Information Disclosure Statement are:

- 1a. ☒ Form PTO-1449.
- 1b. ☒ Copies of IDS citations.
- 1c. ☒ An English language copy of Office Action from a counterpart foreign application.
- 1d. ☐ English language translation (complete or relevant portion(s)) attached to each non-English language publication.
- 1e. ☒ Explanations of Relevancy of References (ATTACHMENT 1(e), hereto) for providing a relevancy of cited documents and concise explanation of each non-English publication.
- 1f. ☐ List of Copending Applications (ATTACHMENT 1(f), hereto).
- 1g. ☒ List of Additional Submitted Documents (ATTACHMENT 1(g), hereto).

2. ☐ This Information Disclosure Statement is filed under 37 CFR §1.97(b):

*(Check either Item 2a or 2b or 2c or 2d)*

- 2a. ☐ Within three months of the filing date of a national application other than a Continued Prosecution Application under § 1.53(d);
- 2b. ☐ Within three months of the date of entry of the national stage as set forth in § 1.491 in an international application.
- 2c. ☐ Before the mailing of a first Office Action on the merits; or
- 2d. ☐ Before the mailing of a first Office Action after the filing of a Request for Continued Examination under § 1.114.

3. ☐ This Information Disclosure Statement is filed under 37 CFR § 1.97(c) after the period specified in paragraph 2 above but before the mailing date of any of a Final Office Action under § 1.113, a Notice of Allowance under § 1.311 or an action that otherwise closes prosecution in the application, AND

*(Check either Item 3a or 3b; Item 3b to be checked if any reference known for more than 3 months)*

3a. ☐ The §1.97(e) Statement in Item 5 below is applicable; OR

3b. ☐ The \$180.00 fee set forth in 37 C.F.R. §1.17(p) is:

☐ enclosed.

☐ to be charged to Deposit Account No. 19-3935.

4. ☒ This Information Disclosure Statement is filed under 37 CFR §1.97(d) after the period specified in paragraph 3 above, but on or before payment of the Issue Fee, AND

4a. ☒ The § 1.97(e) Statement in Item 5 below is applicable; AND

4b. ☒ The \$180.00 fee set forth in 37 C.F.R. §1.17(p) is:

☒ enclosed.

☐ to be charged to Deposit Account No. 19-3935.

5. ☒ Statement under § 1.97(e) (*applicable if Item 3a or Item 4a is checked*)

*(Check either Item 5a or 5b)*

5a. ☒ In accordance with 37 CFR § 1.97(e)(1), it is stated that each item of information contained in this Information Disclosure Statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Information Disclosure Statement.

5b. ☐ In accordance with 37 CFR § 1.97(e)(2), it is stated that no item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in this Information Disclosure Statement was known by any individual designated in §1.56(c) more than three months prior to the filing of this Information Disclosure Statement.

6. ☐ This is a continuation/divisional/continuation-in-part application under 37 CFR § 1.53(b).

*(Check appropriate Items 6a and/or 6b)*

6a. ☐ Copies of the publications listed on the attached Form PTO-1449 which were previously cited in prior application Serial No. \_\_\_, filed on \_\_\_, and which is relied on for an earlier effective filing date for the subject application under 35 U.S.C. § 120, have been omitted pursuant to 37 CFR § 1.98(d).

6b. ☐ Copies of the publications listed on the attached Form PTO-1449 which were not previously cited in prior application Serial No. \_\_\_, filed on \_\_\_, and which is relied on for an earlier effective filing date for the subject application under 35 U.S.C. § 120, are provided herewith.

7. ☐ This is a continuation/divisional application under 37 CFR § 1.53(d) or a Request for Continued Examination under 37 CFR 1.114.

*(Check either Item 7a or 7b)*

- 7a. ☐ The Issue Fee has not been paid.  
7b. ☐ A Petition to Withdraw from issue under 37 CFR § 1.313(c) is filed concurrently herewith or has been granted. A continuation/divisional application under 37 CFR § 1.53(d) or a Request for Continued Examination under 37 CFR 1.114, after payment of the Issue Fee, is proper in accordance with 37 CFR § 1.53(d)(1)(ii) or 37 CFR 1.114(a), respectively.

8. ☐ This is a Supplemental Information Disclosure Statement.

*(Check either Item 8a or 8b)*

- 8a. ☐ This Supplemental Information Disclosure Statement under 37 CFR § 1.97(f) supplements the Information Disclosure Statement filed on \_\_\_\_\_. A bona fide attempt was made to comply with 37 CFR § 1.98, but inadvertent omissions were made. These omissions have been corrected herein. Accordingly, additional time is requested so that this Supplemental IDS can be considered as if properly filed on \_\_\_\_\_.  
8b. ☐ This Supplemental Information Disclosure Statement is timely filed within one (1) month of the Notice under 37 CFR § 1.97 and 1.98, mailed \_\_\_\_\_.

9. ☒ In accordance with 37 CFR § 1.98, a concise explanation of what is presently understood to be the relevance of each non-English language publication is:

*(Check appropriate Items 9a, 9b, 9c and/or 9d)*

- 9a. ☐ satisfied because all non-English language publications were cited on the enclosed "English language version of the search report or action which indicates the degree of relevance found by the foreign office". (See MPEP § 609, Minimum Requirements for an Information Disclosure Statement, Part A(3): Concise Explanation of Relevance, 8th Ed.)  
9b. ☐ set forth in the application.  
9c. ☐ satisfied because an English language translation (complete or relevant portion(s)) is attached to each non-English language publication.  
9d. ☒ enclosed as Attachment 1(e), hereto.


10. No admission is made that the information cited in this Statement is, or is considered to be, material to patentability nor a representation that a search has been made (other than search report(s) from a counterpart foreign application or a PCT International Search Report, if submitted herewith). 37 CFR §§ 1.97(g) and (h).

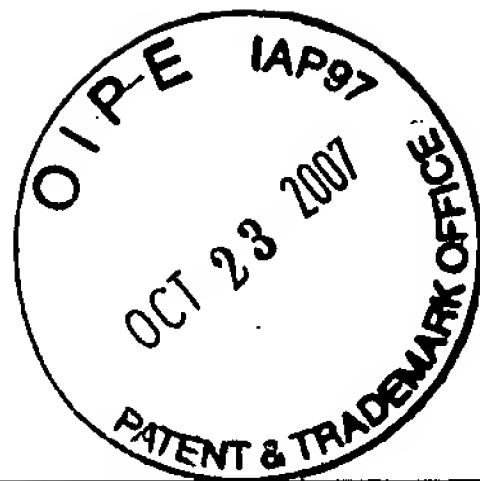
11. The Commissioner is authorized to credit any overpayment or charge any additional fee required under 37 CFR § 1.17 for this Information Disclosure Statement to Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Dated: 1/22/2004  
1201 New York Ave., N.W., Suite 700  
Washington, D.C. 20005  
Telephone: (202) 434-1500  
Facsimile: (202) 434-1501

By:   
Mehdi Sheikerz  
Registration No. 41,307



Sheet 1 of 1

FORM PTO-1449  <b>U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE</b>  <b>LIST OF REFERENCES CITED BY APPLICANT</b>  (Use several sheets if necessary)	ATTORNEY DOCKET NO. 1083.1048	APPLICATION NO. 09/000,924
	FIRST NAMED INVENTOR Takayuki HASEBE et al.	
	FILING DATE December 30, 1997	GROUP ART UNIT 2165

**U.S. PATENT DOCUMENTS**

*EXAMINER INITIAL		DOCUMENT NO.	DATE	NAME	CLASS	SUB- CLASS	FILING DATE
	AA						
	AB						
	AC						
	AD						
	AE						

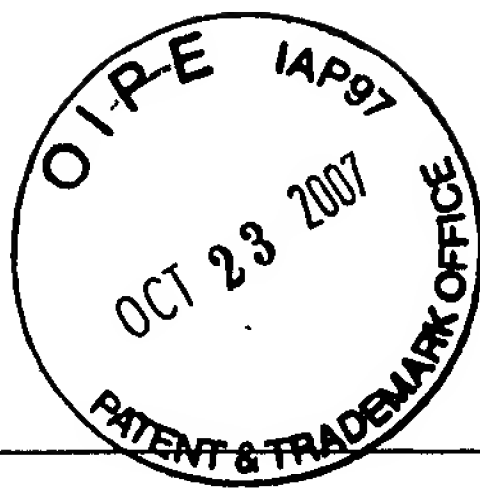
**FOREIGN PATENT DOCUMENTS**

		DOCUMENT NO.	DATE	COUNTRY	CLASS	SUB- CLASS	TRANSLATION YES NO	
	AF	JP 7-30244	11/1995	Japan			In English translated Japanese Office Action	
	AG	JP 8-185448	07/1996	Japan				X
	AH	JP 8-292976	11/1996	Japan				X
	AI	JP 8-329011	12/1996	Japan				X
	AJ	JP 8-255132	10/1996	Japan				X
	AK	JP 3-35351	02/1991	Japan				X

**OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, Etc.)**

			TRANSLATION YES NO	
	AL			

EXAMINER	DATE CONSIDERED
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

**ATTACHMENT 1(e)****EXPLANATIONS OF RELEVANCY  
OF REFERENCES**

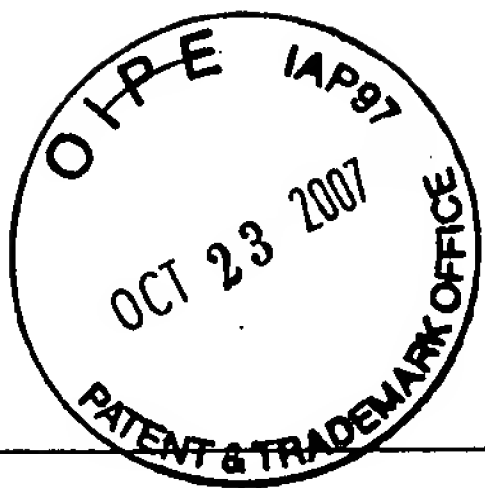
ATTORNEY DOCKET NO. <b>1083.1048</b>	APPLICATION NO. <b>09/000,924</b>
FIRST NAMED INVENTOR <b>Takayuki HASEBE et al.</b>	
FILING DATE <b>December 30, 1997</b>	GROUP ART UNIT <b>2165</b>

The references cited in the attached FORM PTO-1449 hereto were cited in the English translated Japanese Office Action of January 6, 2004 in the counter part Japanese Patent Application No. JP 1997-154046 of the above-identified US patent application.

The Japanese reference cited in item AF of the attached FORM PTO-1449 is explained in the English language translated Japanese Office Action identified in item AE of Attachment 1(g). The remaining five Japanese references of the FORM PTO-1449 were not included in the Reasons for Rejections of the Japanese Office Action (page 3).

Entry and consideration of this Information Disclosure Statement is respectfully requested, pursuant to 37 CFR 1.97(d) and (e)(1) as also specified above in items 4 and 5 of this Information Disclosure Statement.



**ATTACHMENT 1(g)**

<b>LIST OF ADDITIONAL SUBMITTED DOCUMENTS</b>	ATTORNEY DOCKET NO.	APPLICATION NO.
	1083.1048	09/000,924
	FIRST NAMED INVENTOR	
	Takayuki HASEBE et al.	
	FILING DATE	GROUP ART UNIT
	December 30, 1997	2165

The following document(s) is/are listed in accordance with the duty of disclosure provisions of 37 CFR § 1.56, so that the Examiner may consider same should he deem any thereof to be material to examination of the subject application. Pursuant to 37 CFR 1.98(a)(2)(iv), a copy of any identified document(s) is provided.

It is requested that the Examiner acknowledge his consideration of document(s) below-listed by initialing same in the space provided adjacent each such application and that the Examiner sign and date this form at the bottom thereof to confirm such consideration having been given.

This submission in no way represents an admission that any of the information listed herein constitutes prior art with respect to the subject application and unless and until such prior art status is established, this submission is not a request that the information presented herein be printed on the face of any patent issuing from the subject application in which this information is being filed.

**U.S. PATENT DOCUMENTS**

*EXAMINER INITIAL		DOCUMENT NO.	DATE	NAME	CLASS	SUB- CLASS	FILING DATE
	AA						
	AB						

**FOREIGN PATENT DOCUMENTS**

		DOCUMENT NO.	DATE	COUNTRY	CLASS	SUB- CLASS	TRANSLATION YES NO	
	AC							
	AD							

**OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)**

			TRANSLATION YES NO	
	AE	Japanese Office Action in the counter part Japanese Patent Application No. JP 1997-154046, mailed January 6, 2004, including an English translation thereof	X	

EXAMINER	DATE CONSIDERED
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	



OFFICE ACTION

Patent Application No. 1997-154046  
Drafting Date December 22, 2003  
Mailing Date January 6, 2004  
Patent Officer Examiner Motohiro OKUMURA 3044 5N00  
Provisions 29 (2), 36

To Attorney Takao KOHNO et al.

This application is rejected for the following reasons. A response should be filed within sixty days from the mailing date of this Notification.

Reasons

Reason 1

As the inventions of the following claims of this application are not patented because they do not fulfill the requirements of the Patent Law 36(6-ii).

Notes

1.

Claims 1-16

Remarks:

In claim 1, the terms "data" and "input data" are indefinite. In particular, it is impossible to differentiate these two terms, and it is not clear what types of data they are, and hence, it is impossible to know the purpose of the system of the present application.

Reason 2

As the inventions of the following claims of this application are considered such ones that a person with ordinary skill in the art to which the inventions pertain could easily have made prior to the filing of this application on the basis of the inventions described in the following publications issued in Japan or the foreign countries, this application can not be patented according to the Patent Law 29 (2).

Note (As to the references, see the following list thereof)

Claims: 1-16

Cited Reference: 1

Remarks

Cited Reference 1 discloses an invention for editing and storing information on a piece of literary work, comprising various kinds of data including: material data that constitutes each piece of work; quotation data for specifying information on a quoted piece of work and material data of another piece of work; work construction data for issuing instructions for constructing a piece of work on the basis of the material data and the quotation data; and property right data comprising data indicating a rightful claimant of intellectual property right pertain to the piece of work, the amount of value and limitation on use.

In the invention disclosed in Cited Reference 1, it is clear that the quotation data which is protected as intellectual property is not directly stored in the work information, and only work information of the quoted piece of work and data for specifying material data in another piece of work is stored in the work information. It is also clear that accounting is appropriately made upon quotation of the work.

Further, it is a known practice to prevent an unauthorized access to data

for cut-and-paste process.

#### Cited References

1. Japanese Patent Application Laid-Open No. 7-302244

If new reason for rejection is found, the rejection will be notified.

---

#### PRIOR ART SEARCH

A search in Prior Arts was conducted on IPC 7th edition; G06F12/14

Prior Art: Japanese Patent Application Laid-Open No. 8-185448

Japanese Patent Application Laid-Open No. 8-292976

Japanese Patent Application Laid-Open No. 8-329011

Japanese Patent Application Laid-Open No. 8-255132

Japanese Patent Application Laid-Open No. 3-35351

This recordation is not included in the Reason for Rejections.

## CERTIFICATION

I, Kohno Takao; 4-3 Tsurigane-cho, 2-chome, Chuo-ku, Osaka 540-0035 JAPAN, hereby certify that each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement.



KOHNO Takao

Dated this 19th day of January, 2004

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-302244

(43) 公開日 平成7年(1995)11月14日

(51) Int.Cl. <sup>9</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 1 0 U	7459-5L		
1/00	3 7 0 F			
H 0 4 L 12/40				
		9466-5K	H 0 4 L 11/ 00	3 2 1
			11/ 18	
			審査請求 未請求 請求項の数7	FD (全 16 頁) 最終頁に続く

(21) 出願番号 特願平6-113976

(22) 出願日 平成6年(1994)4月28日

(71) 出願人 000002897

大日本印刷株式会社

東京都新宿区市谷加賀町一丁目1番1号

(72) 発明者 伊藤 憲朗

東京都新宿区市谷加賀町一丁目1番1号

大日本印刷株式会社内

(72) 発明者 越智 隆

東京都新宿区市谷加賀町一丁目1番1号

大日本印刷株式会社内

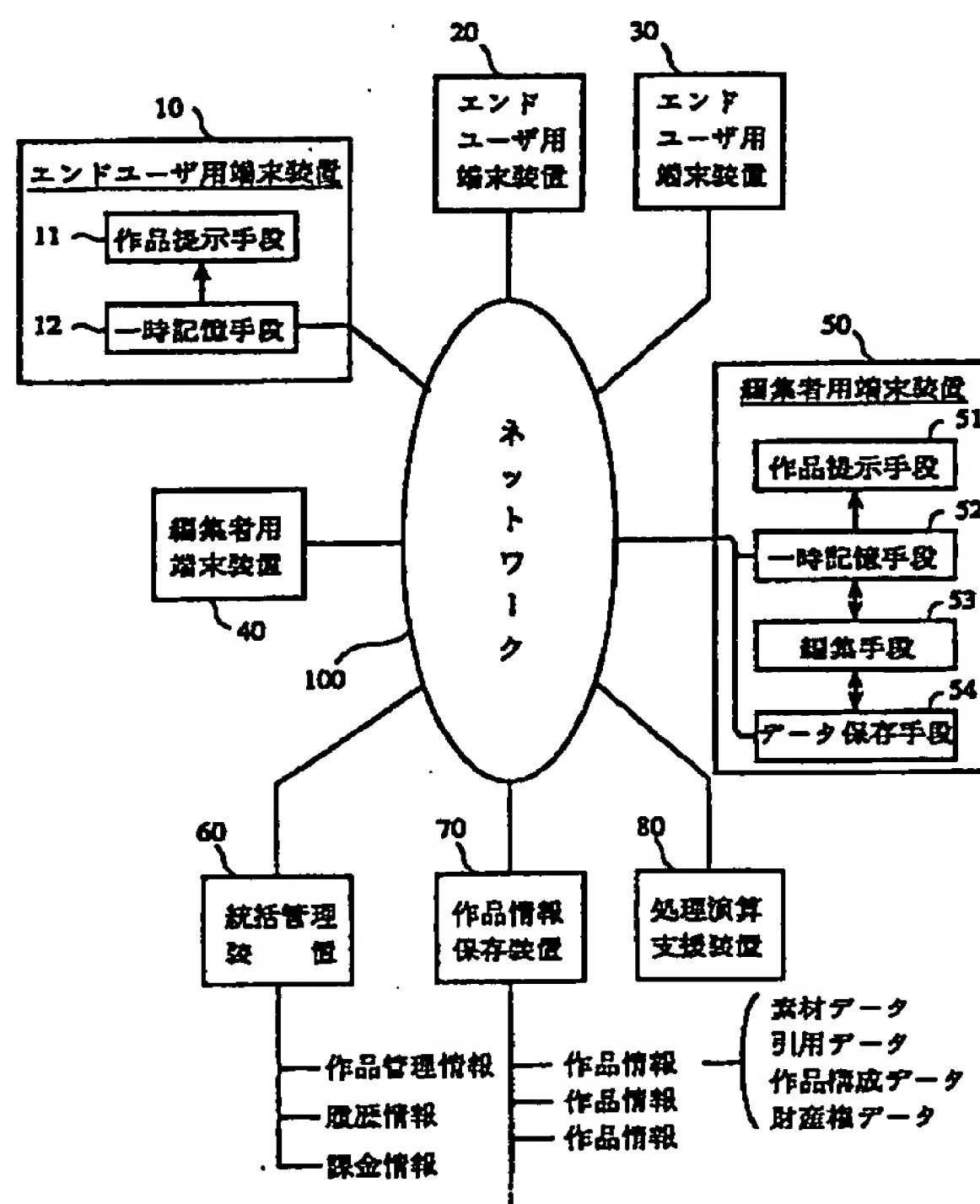
(74) 代理人 弁理士 志村 浩

(54) 【発明の名称】 ネットワークを用いた著作物提供システム

## (57) 【要約】

【目的】 提供した著作物に付随する知的財産権の管理を効率的に行う。

【構成】 ネットワーク100に、端末装置10～50が接続される。統括管理装置60は、このシステム全体を統括管理し、作品情報保存装置70内には、多数のマルチメディア作品が作品情報の形で保存されている。端末装置10からの要求に応じて、作品情報保存装置70から所望の作品情報が伝送される。伝送された作品情報には、その作品の権利者、利用対価、利用制限といった情報を示す財産権データが含まれている。統括管理装置60は、どの端末装置にどの作品情報が提供されたかを示す履歴情報を作成するとともに、提供された作品の財産権データに基づいて、利用者から権利者に対価の支払いが行われるべきことを示す課金情報を作成する。作品情報には他の作品の引用を示す引用データも含まれ、課金情報はこの引用データをも考慮して作成される。



## 【特許請求の範囲】

【請求項 1】 複数の利用者に情報を流すためのネットワークと、  
このネットワークに接続された複数の端末装置と、  
このネットワークを介して提供すべき著作物を、各作品ごとに作品情報として保存する作品情報保存装置と、  
各端末装置に対する作品情報の伝送処理を統括管理する統括管理装置と、  
を備え、

前記作品情報を、単位著作物を構成する素材データと、  
この素材データに基いて作品を構成するための指示を与える作品構成データと、作品に付随する知的財産権の権利者および対価額を示す情報を含む財産権データと、により構成し、

前記端末装置は、前記作品情報内に含まれている素材データで表現される単位著作物を、作品構成データに示されている指示に基いて提示する処理を行い、

前記統括管理装置は、端末装置に作品情報を伝送するときに、この端末装置の利用者に対して、伝送された作品情報内の財産権データに示された対価額を権利者に支払うべきことを示す課金情報を作成する処理を行うことを特徴とするネットワークを用いた著作物提供システム。

【請求項 2】 複数の利用者に情報を流すためのネットワークと、  
このネットワークに接続された複数の端末装置と、  
このネットワークを介して提供すべき著作物を、各作品ごとに作品情報として保存する作品情報保存装置と、  
各端末装置に対する作品情報の伝送処理を統括管理する統括管理装置と、  
を備え、

前記作品情報を、単位著作物を構成する素材データおよび／または引用すべき他の作品情報を特定する引用データと、これらのデータに基いて作品を構成するための指示を与える作品構成データと、作品に付随する知的財産権の権利者および対価額を示す情報を含む財産権データと、により構成し、

前記端末装置は、前記作品情報内に含まれている素材データで表現される単位著作物については、作品構成データに示されている指示に基いて提示し、前記作品情報内に含まれている引用データで表現される著作物については、引用データによって特定される被引用作品についての作品情報を前記ネットワークを介して受け取り、この被引用作品についての作品情報に基いて提示する処理を行い、

前記統括管理装置は、端末装置に作品情報を伝送するときに、この端末装置の利用者に対して、伝送された作品情報内の財産権データに示された対価額を権利者に支払うべきことを示す課金情報を作成する処理を行うことを特徴とするネットワークを用いた著作物提供システム。

【請求項 3】 請求項 1 または 2 に記載のシステムにお

いて、

端末装置には、ネットワークを介して伝送された作品情報を一時的に保持するための一時記憶手段と、この一時記憶手段内に保持されている作品情報に基いて作品を提示するための作品提示手段と、を設け、

ネットワークを介して端末装置に伝送された作品情報のうち、前記作品提示手段による提示が終了した部分については、順次、前記一時記憶手段から消去されるようにしたことを特徴とするネットワークを用いた著作物提供システム。

【請求項 4】 請求項 2 または 3 に記載のシステムにおいて、

ネットワークに接続された複数の端末装置の少なくとも 1 つには、

素材データおよび／または引用データと、作品構成情報とを合成することにより新たな作品を作成し、これに更に財産権データを付加して新たな作品情報を作成し、この新たな作品情報を、前記ネットワークを介して作品情報保存装置に新規保存する処理を行う編集手段を更に設けたことを特徴とするネットワークを用いた著作物提供システム。

【請求項 5】 請求項 1 ～ 4 のいずれかに記載のシステムにおいて、

財産権データ内に示された対価額として、作品の利用態様ごとに異なる額を設定することを特徴とするネットワークを用いた著作物提供システム。

【請求項 6】 請求項 1 ～ 5 のいずれかに記載のシステムにおいて、

財産権データとして、更に、作品の利用態様を制限する条件を付加したことを特徴とするネットワークを用いた著作物提供システム。

【請求項 7】 請求項 1 ～ 6 のいずれかに記載のシステムにおいて、

各端末装置に対して、過去にどの作品情報が伝送されたかを示す履歴情報を、統括管理装置内に蓄積するようにしたことを特徴とするネットワークを用いた著作物提供システム。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】 本発明はネットワークを用いた著作物提供システム、特に、マルチメディアを利用した作品をネットワークを介して提供するとともに、提供した著作物に付随する知的財産権の対価についての課金処理を自動的に行うシステムに関する。

## 【0002】

【従来の技術】 ここ数年、コンピュータ機器のデータ処理能力の向上とともに、画像情報、音声情報、文字情報などを総合的に取り扱ういわゆるマルチメディアの利用が急速に普及してきている。このマルチメディアは、種々の著作物を提供するためのデジタル媒体として、今後

10

20

30

40

50



も広く利用されるものと思われる。このようなマルチメディアを利用した著作物を、一般のユーザに提供する方法として、フロッピディスクや、CD-ROMなどの記憶媒体を用いる方法と、ネットワークを媒介に用いる方法と、が現在普及している。特に、ネットワークを媒介に用いる方法は、データの容器となるべき物理的な記憶媒体を必要としないため、今後も益々広まってゆくものと期待されている。現在では、パーソナルコンピュータの通信機能を利用して、広域の商用ネットワークに容易にアクセスできる環境が整ってきており、マルチメディアを利用した種々の著作物データが、ネットワークを介して個々のパーソナルコンピュータにダウンロードされている。

#### 【0003】

【発明が解決しようとする課題】 前述のように、マルチメディアを利用した著作物の作品は、一般に、画像情報、音声情報、文字情報などを含むものであるが、これら個々の情報も、それぞれ独立した著作物としての作品である。しかも、これら個々の独立した著作物が、すべて一人の著作者の創作によるものであるということはむしろ希であり、今後は、複数の著作者による著作物の集合として、1つのマルチメディア作品が創作されるケースが益々多くなってゆくものと予想される。別言すれば、マルチメディア作品を創作する上で、自分の作品の中に、他人の作品を引用して取り込むという手法が、今後は、ごく一般的に利用されてゆくものと考えられる。

【0004】ところが、個々の著作物には、著作権をはじめとする知的財産権がそれぞれ生じており、他人の著作物を利用するためには、正当な権利者に対してしかるべき対価を支払う必要があり、また、正当な権利者が設定した利用条件を守る必要がある。しかしながら、マルチメディア作品は、上述のように、1つの作品の中に様々な著作物が含まれており、個々の著作物について正当な権利者を特定し、それぞれにしかるべき対価を支払い、利用条件を順守することは、非常に煩雑な作業を強いられることになる。

【0005】そこで本発明は、提供した著作物に付随する知的財産権の管理を効率的に行うことができるネットワークを用いた著作物提供システムを提供することを目的とする。

#### 【0006】

##### 【課題を解決するための手段】

(1) 本発明の第1の態様は、ネットワークを用いた著作物提供システムにおいて、複数の利用者に情報を流すためのネットワークと、このネットワークに接続された複数の端末装置と、このネットワークを介して提供すべき著作物を、各作品ごとに作品情報として保存する作品情報保存装置と、各端末装置に対する作品情報の伝送処理を統括管理する統括管理装置と、を設け、作品情報を、単位著作物を構成する素材データと、この素材デー

タに基いて作品を構成するための指示を与える作品構成データと、作品に付随する知的財産権の権利者および対価額を示す情報を含む財産権データと、により構成し、端末装置は、作品情報内に含まれている素材データで表現される単位著作物を、作品構成データに示されている指示に基いて提示する処理を行い、統括管理装置は、端末装置に作品情報を伝送するときに、この端末装置の利用者に対して、伝送された作品情報内の財産権データに示された対価額を権利者に支払うべきことを示す課金情報を作成する処理を行うようにしたものである。

【0007】(2) 本発明の第2の態様は、ネットワークを用いた著作物提供システムにおいて、複数の利用者に情報を流すためのネットワークと、このネットワークに接続された複数の端末装置と、このネットワークを介して提供すべき著作物を、各作品ごとに作品情報として保存する作品情報保存装置と、各端末装置に対する作品情報の伝送処理を統括管理する統括管理装置と、を設け、作品情報を、単位著作物を構成する素材データあるいは引用すべき他の作品情報を特定する引用データと、これらのデータに基いて作品を構成するための指示を与える作品構成データと、作品に付随する知的財産権の権利者および対価額を示す情報を含む財産権データと、により構成し、端末装置は、作品情報内に含まれている素材データで表現される単位著作物については、作品構成データに示されている指示に基いて提示し、作品情報内に含まれている引用データで表現される著作物については、引用データによって特定される被引用作品についての作品情報をネットワークを介して受け取り、この被引用作品についての作品情報に基いて提示する処理を行い、統括管理装置は、端末装置に作品情報を伝送するときに、この端末装置の利用者に対して、伝送された作品情報内の財産権データに示された対価額を権利者に支払うべきことを示す課金情報を作成する処理を行うようにしたものである。

【0008】(3) 本発明の第3の態様は、上述の第1または第2の態様に係るシステムにおいて、端末装置には、ネットワークを介して伝送された作品情報を一時的に保持するための一時記憶手段と、この一時記憶手段内に保持されている作品情報に基いて作品を提示するための作品提示手段と、を設け、ネットワークを介して端末装置に伝送された作品情報のうち、作品提示手段による提示が終了した部分については、順次、一時記憶手段から消去されるようにしたものである。

【0009】(4) 本発明の第4の態様は、上述の第2または第3の態様に係るシステムにおいて、ネットワークに接続された複数の端末装置の少なくとも1つには、素材データや引用データと、作品構成情報とを合成することにより新たな作品を作成し、これに更に財産権データを付加して新たな作品情報を作成し、この新たな作品情報を、ネットワークを介して作品情報保存装置に新規



保存する処理を行う編集手段を更に設けるようにしたものである。

【0010】(5) 本発明の第5の態様は、上述の第1～第4の態様に係るシステムにおいて、財産権データ内に示された対価額として、作品の利用態様ごとに異なる額を設定するようにしたものである。

【0011】(6) 本発明の第6の態様は、上述の第1～第5の態様に係るシステムにおいて、財産権データとして、更に、作品の利用態様を制限する条件を付加するようにしたものである。

【0012】(7) 本発明の第7の態様は、上述の第1～第6の態様に係るシステムにおいて、各端末装置に対して、過去にどの作品情報が伝送されたかを示す履歴情報を、統括管理装置内に蓄積するようにしたものである。

#### 【0013】

【作 用】本発明のシステムでは、個々のマルチメディア作品（提供すべき著作物）は、ネットワークに接続された作品情報保存装置内に、各作品ごとに作品情報として保存される。ここで、各作品情報は、素材データと、引用データと、作品構成データと、財産権データと、により構成されている。素材データは、実際の著作物データそのものからなる生のデータであるが、引用データは、引用すべき他の作品を特定するためのデータであり生のデータは含まない。一方、財産権データは、この作品に付随する知的財産権の権利者および対価額を示す情報を含んでいる。また、作品構成データは、素材データあるいは引用データに基いて、実際の作品を構成するための指示を与えるデータであり、端末装置は、この作品構成データの指示に基いて、ネットワークを介してリアルタイムで伝送されてくる素材データあるいは引用データに基く作品の提示を行う。すなわち、伝送されたデータが素材データの場合には、作品構成データで指示されるレイアウト位置、割付倍率、タイミング、などに従ってリアルタイムでの提示が行われ、伝送されたデータが引用データの場合には、この引用データによって特定される被引用作品についての作品情報が、新たにネットワークを介して伝送される。

【0014】しかも、このシステムには、ネットワーク上での情報の流れを統括管理する統括管理装置が設けられており、どの端末装置にどの作品情報が伝送されたか、という情報がすべて把握される。個々の作品情報には、その作品の権利者および対価額を示す財産権データが含まれているので、ある作品情報がある端末装置へ伝送された場合、統括管理装置では、この財産権データに基いて、伝送先の端末装置の利用者に対して、所定の対価を所定の権利者に支払うべきことを示す課金情報を作成することができる。このように、ネットワーク上を作品情報が伝送されるたびに、統括管理装置内で課金情報の作成が行われるので、対価の支払い処理を効率的に行

うことが可能になる。

【0015】また、作品Aの中で、他人の作品Bが引用されているような場合であっても、作品Aの作品情報内には、作品Bを構成する生のデータは含まれておらず、作品Bを引用することを示す引用データだけが含まれている。したがって、作品Aを端末装置側で再生する場合には、作品Aの作品情報がネットワークを通じて伝送されるとともに、作品Bの作品情報もネットワークを通じて伝送されることになる。そして、作品Aの作品情報が伝送されるときには、その中の財産権データに基いて、作品Aの著作権者に対して支払うべき対価が課金され、作品Bの作品情報が伝送されるときには、その中の財産権データに基いて、作品Bの著作権者に対して支払うべき対価が課金される。このように、1つの作品について多数の知的財産権が発生していた場合であっても、個々の著作権者に対する対価の支払い処理がそれぞれ別個に行われることになる。

【0016】また、従来の一般的なネットワークを用いた著作物提供システムでは、端末装置側において所望の作品を再生する場合、まず、ネットワークを介して個々の著作物データを端末装置側の記憶装置に一旦ダウンロードし、このダウンロードした著作物データをあらかじめディスプレイ画面などに再生するという処理を行っている。このため、再生が終了した後も、ダウンロードしたハードディスク装置などに著作物データは残っている。したがって、この著作物データを不正に複製して、海賊版として販売するような侵害行為が行われやすい。ところが、本発明に係るシステムでは、一般のエンドユーザーに対しては、ダウンロードという手法を用いずに、ネットワークを介して伝送された著作物データを、そのままリアルタイムで提示してしまうという手法を採ることができる。このような手法では、ネットワーク上を伝送されてきた著作物データは、ユーザーに提示された後は、端末装置側には残らないことになる。したがって、知的財産権を侵害する行為を抑制することができる。

【0017】また、ネットワークに接続された端末装置に、更に編集手段を付加しておけば、この編集手段において新たな作品を作成し、この新たな作品についての作品情報を、作品情報保存装置に新規保存する処理が可能になる。このとき、所望の対価額を示す財産権データを付加しておけば、将来、この新たな作品を誰かが利用した場合には、自動的に対価の支払いがなされることになる。更に、作品の利用態様ごとに異なる対価額を設定したり、作品の利用態様を制限する条件を財産権データに盛り込むようにすれば、より効率的な知的財産権管理が可能になる。

#### 【0018】

##### 【実施例】

<システムの基本構成>以下、本発明を図示する実施例に基いて説明する。図1は、本発明の一実施例に係るネ

ットワークを用いた著作物提供システムの基本構成を示すブロック図である。この実施例のシステムでは、ネットワーク100に、エンドユーザ用端末装置10、20、30と、編集者用端末装置40、50と、統括管理装置60と、作品情報保存装置70と、処理演算支援装置80と、が接続されている。これら各装置は、いずれもコンピュータを含んだ装置である。もっとも、この実施例に示すシステムは、説明の便宜上、非常に単純化したモデルを示すシステムであり、実際には、より多数の端末装置が接続されることになる。

【0019】エンドユーザ用端末装置10、20、30としては、この実施例では、汎用のパーソナルコンピュータを用いている。ただ、このシステムの一要素として機能するようにするため、各パーソナルコンピュータには、専用のアプリケーションソフトウェアがインストールされている。あるいは、パーソナルコンピュータのかわりに、テレビゲーム装置などを用いてもかまわない。一方、編集者用端末装置40、50としては、この実施例では、汎用のワークステーションを用いている。後述するように、この実施例で用いられているエンドユーザ用端末装置10、20、30は、著作物データの提供を受ける受動的な機能しか有しないが、編集者用端末装置40、50は、この受動的な機能に加えて、新たな著作物データを編集作成する能動的な機能をも有する。このため、パーソナルコンピュータよりも高い機能をもったワークステーションが用いられている。統括管理装置60は、このシステム全体を統括管理する機能を有する大型コンピュータであり、どのような情報がどの端末装置に伝送されたかという履歴情報を保存する機能を有するとともに、本発明の特徴である課金情報の作成処理を行う機能を有する。また、作品情報保存装置70は、このシステムで利用される著作物データを収容したり配信したりして、一元管理する大型コンピュータであり、著作物データは各作品ごとに作品情報として保存される。作品情報保存装置70内における各作品情報の収容先を示す情報は、統括管理装置60内に作品管理情報として用意される。なお、この実施例では、作品情報保存装置を単一のコンピュータにより構成しているが、複数台のコンピュータで構成してもよい。処理演算支援装置80は、後述するように、作品情報保存装置70内の作品情報を各端末装置へ伝送するときに処理演算を支援する機能を有する大型コンピュータである。

【0020】なお、この実施例のシステムでは、ネットワーク100として、B-ISDN通信回線網を用いており、ネットワーク上を伝送するデータは、ATM交換機群によって処理される。このシステムを商業的に利用するには、たとえば、次のような利用形態を一例として掲げることができる。すなわち、統括管理装置60および処理演算支援装置80を、このシステムを課金処理を含めて統括管理する大手企業に設置し、作品情報保存装

置70を大手の出版社、通信社、プロダクションなどに設置する。そして、編集者用端末装置40、50を、中小の情報提供会社やマルチメディア作品制作会社に設置し、エンドユーザ用端末装置10、20、30を一般のエンドユーザ（企業、個人）に設置する。この場合、統括管理装置60を有する大手企業は、このシステムの課金処理および統括管理を事業として行い収益を得ることができ、作品情報保存装置70を有する大手の出版社、通信社、プロダクションなどは、自社の著作物をマルチメディア作品として提供したり、他社に二次的利用を許可したりして、著作権収益を得ることができ、中小の情報提供会社やマルチメディア作品制作会社は、作品情報保存装置70内の著作物を利用した二次的著作物を提供することにより著作権収益を得ることができる。そして、一般のエンドユーザは、所定の対価を支払うことにより、エンドユーザ用端末装置を用いてマルチメディア作品を鑑賞したり、これに付帯する通信販売などのサービスを受けたりする恩恵に預かれる。

【0021】後述するように、統括管理装置60には、過去に各端末装置に伝送された作品情報の履歴が履歴情報として保存され、この履歴情報に関連して課金情報が作成される。この課金情報は、作品の提供を受けた端末装置の利用者に対して所定の料金を課金することを示す情報であり、より具体的には、支払うべき対価の額と、その相手先（権利者）を示す情報である。したがって、この課金情報に基づいて、たとえば、エンドユーザと権利者との間で銀行口座による決済を行うようにすれば、エンドユーザは料金の支払いを銀行引き落としという形にして、このネットワークによる著作物提供システムを利用することができる。また、このシステムを統括管理する大手企業は、統括管理装置60内に蓄積された履歴情報により副次的なメリットも得られる。すなわち、この履歴情報は、各ユーザが過去にどのような作品をアクセスしたかという事実を示すものであり、ユーザの趣味、嗜好、生活環境などを把握する上で貴重なデータとなる。したがって、種々の商品の販売促進用の情報としても大いに利用できる。

【0022】作品情報保存装置70内に保存される個々の作品情報は、素材データ、引用データ、作品構成データ、財産権データといった各種データによって構成される。ここで、素材データとは、単位著作物（ひとまとまりとして取り扱われる何らかの著作物）を構成する生のデータであり、たとえば、1枚の静止画であればラスターデータの形式の画像データ、動画であればこのような静止画の集合データ、1枚の線画であればベクトルデータの形式の画像データ、ひとまとまりの文章であればJIS漢字コードなどで表現されたテキストデータ、音声であれば所定周期でサンプリングした一連の音圧値データ、ということになる。一方、引用データとは、引用すべき他の作品（被引用作品）の作品情報または他の作品

中の素材データを特定するデータであり、たとえば、個々の作品情報にユニークな識別番号を付与して管理した場合には、被引用作品の作品情報に付与された識別番号が引用データになる。また、作品構成データは、素材データや引用データに基いて、作品を構成するための指示を与えるデータである。たとえば、1枚の静止画からなる素材データと、1枚の線画からなる素材データと、の2つの素材データから1つの作品が構成されている場合、各素材データをディスプレイ画面上のどの位置に、どのような倍率でレイアウトするか、という指示を与えるデータが、作品構成データとなる。また、財産権データは、本発明の特徴となるデータであり、作品に付随する知的財産権（著作権が代表的な権利となるが、特許権などの工業所有権が含まれる場合もありうる）の権利者、対価額、利用制限を示すデータから構成される。

【0023】作品情報保存装置70内の作品情報は、ネットワーク100を介してエンドユーザ用端末装置10、20、30、あるいは編集者用端末装置40、50に伝送される。エンドユーザ用端末装置10には、作品提示手段11と一時記憶手段12とが備わっており、ネットワーク100を介して伝送された作品情報は、一時記憶手段12に一時的に保持され、この一時記憶手段12内に保持されている作品情報に基いて、作品提示手段11によって作品が提示される。この作品提示の処理動作については、後に具体例に即して詳述する。また、同様に、編集者用端末装置50にも、作品提示手段51および一時記憶手段52が備えられており、ネットワーク100を介して伝送された作品情報は、一時記憶手段52に一時的に保持され、この一時記憶手段52内に保持されている作品情報に基いて、作品提示手段51によって作品が提示される。なお、一時記憶手段12、52における作品情報の記憶は、いわゆるダウンロードとは異なり、作品提示手段11、51での作品提示に必要な時間だけの一時的な記憶であり、作品の提示が終了すると、その終了した部分についての作品情報は、順次、消去されることになる。この実施例では、一時記憶手段12、52は揮発性メモリ（RAM）が用いられており、エンドユーザ用端末装置10や編集者用端末装置50の電源をOFFにすると、作品情報はすべて失われることになる。

【0024】編集者用端末装置50内には、更に、編集手段53およびデータ保存手段54が設けられている。編集手段53は、素材データや引用データを用いて新たな作品を作成する機能を有し、この新たな作品についての作品情報は、ネットワーク100を介して作品情報保存装置70内に新規保存させることができる。また、データ保存手段54は、伝送されてきた作品情報をダウンロードするための手段である。前述のように、端末装置側において作品提示を行う場合には、作品情報は一時記憶手段52内に一時的に記憶され、作品提示手段51に

より提示が終了すると消去される。これに対して、ダウンロードを行った場合には、作品情報はデータ保存手段54内に保存され、作品の提示が終了した後も、本願発明に係るシステムの外部の作品として、編集作業などに利用できる。

【0025】＜作品情報の具体例＞以上、このシステムの基本構成を説明したが、続いて、このシステムで用いる作品情報の内容を、具体例に即して説明する。一般に、マルチメディア作品は、動画、静止画、文字、図形、音声などの素材を組み合わせて構成されており、ディスプレイ装置およびスピーカによってユーザに提示されることになる（もっとも、マルチメディア作品は、視覚あるいは聴覚によって鑑賞されるものに限定されず、触覚、味覚、嗅覚によって鑑賞されるものも含まれ、触感再生機などによっても提示可能である。）。ここでは、図2に示すような作品を例にとりて、作品情報の内容説明を行うことにする。図2は、この作品のディスプレイ画面上での表示態様を示したものである。なお、本明細書において「作品」という文言は、いわゆる芸術的な絵画、音楽といった作品だけに限定されるものではなく、ひとつのまとまった表現として認識できる著作物を広く含む意味で用いている。たとえば、図2に示す作品は、「日米貿易摩擦」という作品名が付けられており、芸術作品というよりは、ニュース、ドキュメンタリー、解説記事、といった性質の著作物である。

【0026】さて、この図2に示す画面は、画面右上部分にレイアウトされた標題ロゴ1（テキストおよびラスターデータで表現された静止画）と、その下にレイアウトされた本文記事2（テキストデータ）と、画面左上部分にレイアウトされた映像3（ラスターデータで表現された複数枚の静止画（フレーム）の集合からなる動画データ、なおこの動画に同期して音声も再生される）と、その下にレイアウトされた2つの制御ボタン4、5とによって構成されている。この作品を提示させたときの初期状態では、映像3は最初のフレームのみが表示された静止状態になっている。ここでユーザが、制御ボタン4をクリックすると（たとえば、マウスポインタをこのボタンの位置まで動かして、マウスボタンを押すような操作を行う）、映像3としての動画および音声の再生がスタートする。後述するように、この映像自身は、「Mr. Kのインタビュー」という作品名が付された1つの独立した作品であり、日米貿易摩擦に関してのMr. Kに対するインタビューの模様を収録したものである。すなわち、「日米貿易摩擦」という作品の一部において、「Mr. Kのインタビュー」という別な作品が引用されていることになる。この映像3の再生が終了すると、画面上では最後のフレームが表示された静止状態になり、更に、これまでは表示されていなかった略歴6が表示されるようになる。この略歴6は、Mr. Kの略歴を示すテキストデータである。



【0027】一方、ユーザが、制御ボタン5をクリックすると、図3に示すように、映像3がレイアウトされていた領域に、グラフ7が表示されるようになる。このグラフ7は、ベクトルデータで表現された静止画である。グラフ7が表示されると同時に、制御ボタン5は制御ボタン8に置き変わる。この図3の状態において、ユーザが、制御ボタン4をクリックすると、再び図2の表示状態に戻り、映像3の再生がスタートする。また、図3の状態において、ユーザが制御ボタン8をクリックすると、この作品の提示は終了し、別な作品を選択するためのモードに移行することになる。

【0028】このように、マルチメディア作品は、動画、静止画、テキスト、音声など様々なジャンルの著作物を組み合わせて構成されており、ユーザとの間でインタラクティブ方式（対話方式）で作品の提示が進行するのが一般的である。しかも、上述の例のように、別な作者による作品を引用することも行われ、知的財産権の権利関係は非常に複雑になる。たとえば、上述の例では、「日米貿易摩擦」なる作品の提供を受けたユーザは、この作品の作者に対して対価を支払う義務が生じるとともに、その中で引用されている「Mr. Kのインタビュー」なる作品の作者に対しても対価を支払う義務が生じることになる。上述の例は、1つの作品内で1つの引用だけが行われている非常に単純なモデルであるが、実際には、このような引用が各箇所で行われたり、いわゆる「入れ子」式の多重引用が行われたりするケースが今後は益々増えるものと予想される。このような複雑な引用が行われている作品の提供を受けた場合、知的財産権の管理は非常に複雑にならざるを得ない。

【0029】本システムでは、次のような手法を採ることにより、このような知的財産権管理の問題を解決している。本システムで利用される個々の作品情報は、図4に示すように、内容リスト、素材データ、引用データ、作品構成データ、財産権データによって構成されている。ここで、素材データおよび引用データは、必ずしも両方が必要なものではなく、少なくともいずれか一方があれば足りる。内容リストは、この作品で用いられている素材データおよび引用データの一覧表を示すものであり、作品構成データは、この素材データや引用データに基づいて作品を構成するための指示を与えるものである。また、財産権データは、この作品に係る知的財産権の権利者、利用を行う場合の対価額、利用制限、を示す情報（必要に応じて、時間的な利用制限やその場合の対価額を含めてもよい）からなる。

【0030】図2および図3に示した作品「日米貿易摩擦」についての作品情報の構成を図5に示す。内容リストには、この作品が素材データA、B、Cと、引用データDとを含むことが示されており、素材データA～Cとしては、生の画像データあるいはテキストデータが収容されている。また、引用データDとしては、「Mr. K

のインタビュー」なる作品を特定するデータ（たとえば、固有の識別番号）が収容されている。作品構成データは、各素材データA～Cのレイアウト位置や倍率を指示するデータ、制御ボタン4、5のパターン、レイアウト位置、機能を指示するデータ、全体の合成手順や同期指定を指示するデータ、などからなる。そして、財産権データとしては、権利者は「甲」、対価額は「再生利用した場合に20円」、利用制限は「ダウンロード不可、素材データAのみの単独引用不可」なる情報が記述されている。

【0031】一方、この作品「日米貿易摩擦」において引用されている別な作品「Mr. Kのインタビュー」についての作品情報の構成を図6に示す。内容リストには、この作品が素材データE、Fを含むことが示されており、素材データE、Fとしては、生の画像データあるいはテキストデータが収容されている。作品構成データは、各素材データE、Fのレイアウト位置や倍率を指示するデータ、全体の合成手順や同期指定を指示するデータ、などからなる。そして、財産権データとしては、権利者は「乙」、対価額は「再生利用した場合に5円、ダウンロード利用した場合に500、000円」、利用制限は「部分引用不可」なる情報が記述されている。

【0032】以上、作品情報の具体例を、2つの作品について示したが、要するに、動画、静止画、図形、テキスト、音声、などマルチメディアの対象となる素材を表わす生のデータである素材データか、あるいは、引用すべき別な作品を特定するための引用データを用いて作品を構成し、構成指示を与えるための作品構成データおよび知的財産権に関する情報を示す財産権データを付加した形式になっていれば、本発明における作品情報としての条件を備えることになる。なお、上述の具体例では、いずれも複数の素材データを用いた作品となっているが、単一の素材データあるいは単一の引用データによって、作品を構成することももちろん可能である。また、各素材データには、動画、静止画、図形、テキスト、音声、といった生のデータに、これら生のデータに対して施す加工処理を示すデータを付加しておくこともできる。たとえば、カラー画像の場合は、色調整を行うための条件や、特殊画像効果を施すための条件を加工処理データとして付加しておけば、端末装置側では、加工後のデータを再生することができる。また、素材としての画像データの一部分のみを用いるような場合にも、カットやトリミングを施すための加工処理データを付加しておけば、再生時に必要な部分のみを提示することができる。もちろん、このような加工処理データ自身も著作物のひとつであり、利用に際しては対価を要求することができる。

【0033】また、各作品情報には、出力フォーマット情報を付加しておくことと便利である。現在、種々のパーソナルコンピュータが普及しており、マルチメディア作品

を再生するソフトウェアの規格も種々のものが採用されている。そこで、各作品ごとに出力フォーマット情報を付加しておけば、個々の端末装置において適応可能なフォーマットか否かを直ちに判断することができ、必要があれば所定のフィルタを通してフォーマット変換を行い、異なるフォーマットをもった作品にも適応させるような処理が可能になる。

【0034】＜端末装置における提示処理＞続いて、端末装置側における各作品の提示処理を、具体例に即して説明する。図1において、エンドユーザ用端末装置10が作品提示手段11と一時記憶手段12とによって構成されていることを示した。この作品提示手段11および一時記憶手段12は、エンドユーザ用端末装置10を機能面からみた場合のブロック構成要素である。図7に示すブロック図は、この端末装置10をハードウェア構成面からみた場合のブロック構成要素を示している。前述のように、実際には、このエンドユーザ用端末装置10は、汎用のパーソナルコンピュータやテレビゲーム装置から構成されている。すなわち、ネットワーク100に対して、ターミナルアダプタ101を介して演算処理装置102が接続されており、この演算処理装置102には、作品を提示するためのディスプレイ装置103およびスピーカ104が接続されている。また、演算処理装置102には、不揮発性メモリとしてのROM105と、揮発性メモリとしてのRAM106（VRAMも含む）が接続されており、更に、記憶装置としてディスク装置107が接続されている。このディスク装置107内には、本システムのアプリケーションソフトウェア

（この汎用パーソナルコンピュータを、本システムの構成要素である端末装置10として動作させるためのプログラム、別言すれば、ネットワーク100から送信されてくる、端末装置の機種に依存しない汎用のデータを、その端末装置の方式に合致させて所定の処理を実行させるためのプログラム）と、他のアプリケーション

（汎用パーソナルコンピュータで利用されているワードプロセッサ、スプレッドシート、CAD、などのプログラムで、本発明の実施には必要はない）と、がインストールされている。また、演算処理装置102に対して、ユーザが所定の情報入力を行うための装置として、キーボード108およびマウス109などが接続されている。

【0035】さて、このような端末装置10を用いて、図5に示すような作品情報をもった「日米貿易摩擦」なる作品を再生する場合の動作を説明しよう。この作品情報は、作品情報保存装置70内にデータベースとして保存されているが、端末装置10側からこの作品の伝送を要求すると、統括管理装置60の管理のもとに端末装置10が作品情報保存装置70に接続され、ネットワーク100を介して端末装置10に、この作品情報が伝送される。ただし、全データがすべて伝送されるわけではな

い。ここが従来のシステムにおけるダウンロードとは異なる点である。はじめに、内容リストと作品構成データとが伝送され、RAM106内に格納される。このRAM106内に格納された情報に基づいて、本システムのアプリケーションプログラムは、この作品についての概要を認識することができる。この内容リストおよび作品構成データは、生の素材データに比べると、非常に小規模なデータであり、比較的小さな容量のメモリで格納できる。

【0036】続いて、このアプリケーションプログラムは、作品構成データの指示に基づいて、この作品の再生を行う。作品構成データ内には、まず、図2に示すような画面表示を行うための手順が記述されている。このような画面表示を行うために必要なデータは、標題ロゴ1の画像データ（素材データA）、本文記事2のテキストデータ（素材データB）、映像3の初期画面の画像データ（引用データDによって引用指定された「Mr. Kのインタビュー」なる作品内の素材データEの1フレーム目）、そして、制御ボタン4、5に関するデータである。そこで、アプリケーションプログラムは、統括管理装置60に対して、素材データAおよびB、ならびに、別な作品情報内の素材データEの1フレーム目、を伝送するよう要求を出す。統括管理装置60は、この要求に基づいて、端末装置10を作品情報保存装置70に接続し、端末装置10に対して作品情報保存装置70内の素材データA、B、Eにアクセスする許可を与える。一方、統括管理装置60から作品情報保存装置70に対しては、素材データA、B、Eを送信する命令が与えられる。かくして、端末装置10からのアクセスにより、素材データA、B、Eが伝送されることになる。これらのデータは、端末装置10側に伝送されてくると、RAM106内（より詳しくは、VRAM内）に一時的に保持される。このとき、各素材のレイアウト位置や倍率は、作品構成データ内の指示に基づいて決定される。

【0037】かくして、図2に示すような画面が、ディスプレイ装置103に表示されることになる。なお、制御ボタン4、5は、作品構成データ内に含まれているデータに基づいて作成される。ここで、ユーザが、マウス109を用いて制御ボタン4をクリックし、映像3の再生を開始させる指示を与えたとする。すると、アプリケーションプログラムは、作品情報保存装置70に対して、引用データDで特定された「Mr. Kのインタビュー」なる作品の作品情報を伝送するよう要求を出す。この結果、「日米貿易摩擦」という作品中に引用された形で、「Mr. Kのインタビュー」なる作品が提示されることになる。すなわち、ディスプレイ装置103の画面上で、図2に示すような映像3が音声とともに再生されることになる。再生が終了したときには、素材データFが伝送され、略歴6が表示されることになる。

【0038】ここで重要な点は、RAM106上に伝送

されてきた素材データは、ディスプレイ装置103およびスピーカ104における提示(再生)処理に必要な間だけ一時的に保持されているだけであり、それ以後は随時消去されるという点である。具体的には、映像3の各フレームを構成する画像データは、現在表示中の1フレーム分が最低限残されていけばよい。結局、ネットワーク100を介して伝送されてきた素材データは、提示後に消去されることになる。もっとも、提示が終了したデータを、必ずしも即座にRAM106内から消去する必要はない。RAM106の残り容量などを考慮して、新たな素材データを格納する十分なスペースが確保できるように、適宜、不要なものを消去してゆけばよい。このように、素材データを提示処理後に適宜消去する主眼は、RAM106の容量を節約することと、素材データの不正利用を阻止することにある。このシステムを動作させるためのアプリケーションプログラムの終了時には、素材データをすべてRAM106上から消去するようにしておけば、素材データがこのシステムの閉鎖系から外部へ漏洩することがなく、不正利用を阻止することができるのである。

【0039】ここで、ユーザが、マウス109を用いて制御ボタン5をクリックし、グラフ7の提示をさせる指示を与えたとする。すると、アプリケーションプログラムは、作品情報保存装置70に対して、素材データCを伝送するよう要求を出す。こうして、RAM106内に素材データCが伝送されると、図3に示すように、ディスプレイ装置103の画面上にグラフ7が表示される。この時点では、RAM106内の素材データE、Fは消去されていてかまわない。もし、ユーザが制御ボタン4をクリックして、再び、映像3の再生を要求した場合には、作品情報保存装置70から、素材データE、Fの伝送が再度行われることになる。この実施例では、ネットワーク100として、B-ISDN通信回路網を用いているため、データの高速度伝送が可能である。したがって、映像3を再生する旨の指示がユーザから与えられるたびに、素材データE、Fをネットワークを介して伝送し、これをディスプレイ装置103上に表示するという手法を採っても、時間的な遅れが生じることはなく、伝送された素材データをリアルタイムで再生することが可能である。

【0040】<システム全体の動作>続いて、図1に示すシステム全体の動作を、図8の流れ図に基いて説明する。いま、エンドユーザ用端末装置10からユーザが、このシステムにアクセスを開始したものとしよう。すなわち、このユーザは、端末装置10として用いている汎用パーソナルコンピュータにおいて、本システムのアプリケーションプログラムを立ちあげたことになる。端末装置10からのアクセスが開始されたことは、統括管理装置60において認識される。そこで、統括管理装置60は、ステップS1において、端末装置10に対して作

品リストの提示を行う。すなわち、作品情報保存装置70内に用意されている種々の作品情報のリストが端末装置10に伝送される。ユーザは、ステップS2において、このリストの中から鑑賞したい作品を選択する指示を入力する。たとえば、前述した「日米貿易摩擦」なる作品が選択されたものとしよう。続く、ステップS3では、統括管理装置によるアクセス許可が行われる。すなわち、統括管理装置60から作品情報保存装置70に対して、端末装置10からの「日米貿易摩擦」なる作品に対するアクセスを許可する旨の通告が行われる。同時に、選択された作品についての財産権データが統括管理装置60に読み込まれる。ここで、統括管理装置60は、「日米貿易摩擦」なる作品が端末装置10に伝送されたことを示す履歴情報を作成するとともに、端末装置10の利用者に対して所定の対価を課すための課金情報を作成する。具体的には、図5の作品情報に示されているように、この作品についての財産権データによれば、権利者は「甲」で再生利用(データを単に再生して鑑賞するだけの利用態様)の対価額は「20円」となっているので、端末装置10の利用者に対して、甲に20円を支払うべきことを示す課金情報が作成されることになる。

【0041】次に、ステップS4において、選択された作品についての内容リスト、作品構成データ、財産権データの取込みが行われる。すなわち、これらのデータが、端末装置10内のRAM106に取り込まれる。

【0042】続いて、ステップS5では、端末装置10内で次に行うべき提示処理が、作品構成データに基づいて認識される。たとえば、「日米貿易摩擦」なる作品が選択された場合には、まず、図2に示す標題ロゴ1の提示処理が、さしあたって行うべき処理として認識される。標題ロゴ1は素材データAとして与えられるので、ステップS6からステップS7へと分岐し、支援処理(後述)が必要であればステップS8における支援処理を経てステップS9に進み、素材データAの取込みおよび提示処理が実行される。こうして、素材データAにより標題ロゴ1の提示が完了したら、ステップS10からステップS5へと戻り、次に行うべき処理として、本文記事2の提示処理が認識される。そこで、ステップS6からステップS7へと分岐し、やはり支援処理が必要であればステップS8における支援処理を経てステップS9に進み、素材データBの取込みおよび提示処理が実行される。こうして、素材データBにより本文記事2の提示が完了したら、ステップS10からステップS5へと戻り、次に行うべき処理として、映像3の提示処理が認識される。この映像3は、引用データDによって与えられているので、ステップS6からステップS11へと分岐し、被引用作品の選択が行われる。この例の場合、引用データDによって特定される被引用作品として、「M r. Kのインタビュー」が選択される。なお、上述した



個々の提示処理は、プリエンティティブ・マルチタスクによるマルチプロセス間通信などの手法により、同時に実行することも可能である。また、分散オブジェクトプロセス技術を用い、処理演算支援装置 80 で外部処理を同時実行することも可能である。

【0043】こうして、ステップ S 11 において、新たな作品が選択されると、ステップ S 12 における再帰処理が行われる。この再帰処理は、ステップ S 3 からの手順を繰り返し実行する処理であるが、この処理ルーチンは、一階層下のレベルに相当するいわば「入れ子」になったルーチンであるため、図 8 では、ステップ S 12 からステップ S 3 への過程を破線で示してある。この「入れ子」のルーチン内でも、上述した手順と同じ手順が実行され、素材データ E、F の提示が行われることになる。すなわち、ステップ S 3 において、「Mr. K のインタビュー」なる作品についてのアクセスが許可され、統括管理装置 60 において履歴情報および課金情報が作成される。ここで作成される課金情報は、「Mr. K のインタビュー」なる作品についての課金情報である。具体的には、図 6 の作品情報に示されているように、この作品についての財産権データによれば、権利者は「乙」で再生利用の対価額は「5 円」となっているので、端末装置 10 の利用者に対して、乙に 5 円を支払うべきことを示す課金情報が作成されることになる。続いて、ステップ S 5 以下の処理により、「Mr. K のインタビュー」なる作品の提示が完了すると、ステップ S 10 において、全処理完了となりこの手順は終了する。ただ、ここで終了した手順は、「入れ子」になった「Mr. K のインタビュー」なる作品の提示処理であり、実際には、一階層上のレベルのものの処理ルーチン（「日米貿易摩擦」なる作品の提示処理ルーチン）のステップ S 12 内の再帰処理として実施された手順である。したがって、「Mr. K のインタビュー」なる作品の提示が完了したということは、ステップ S 12 の再帰処理が完了したということである。

【0044】この時点では、ディスプレイ画面上には図 2 に示すような画像表示がなされていることになる。そこで、ステップ S 10 からステップ S 5 へと戻り、図 2 の画面に示す制御ボタン 4、5 がクリックされるのを待つ待機状態になる。ここで、制御ボタン 4 がクリックされれば、再びステップ S 6 からステップ S 11 へと分岐して、引用作品である「Mr. K のインタビュー」の提示が行われる。また、制御ボタン 5 がクリックされれば、ステップ S 6 からステップ S 7 へと分岐し、ステップ S 9 において素材データ C の取り込み提示処理が行われ、グラフ 7 が提示された図 3 に示す画面表示が得られる。こうして、再びステップ S 5 に戻って、制御ボタンのクリック待機状態となる。この「日米貿易摩擦」なる作品は、図 3 の画面に示す制御ボタン 8 がクリックされると終了する。制御ボタン 8 がクリックされた場合は、

提示対象がないので、ステップ S 6 からステップ S 10 へと進み、ここで全処理完了と判断されて、この作品の提示はすべて完了する。

【0045】ここで、端末装置 10 の利用者が、「日米貿易摩擦」なる作品を再生利用した場合に、統括管理装置 60 で行われる課金処理を整理してみる。上述したように、まず、「日米貿易摩擦」なる作品についてのデータがステップ S 3 において取り込まれると、ステップ S 4 において、甲に 20 円を支払うべきことを示す課金情報が作成される。続いて、この作品内で引用されている「Mr. K のインタビュー」なる作品についてのデータがステップ S 3（ステップ S 12 の再帰処理によって実行された一階層下のレベルの処理手順におけるステップ S 3）において取り込まれると、続くステップ S 4 において、乙に 5 円を支払うべきことを示す課金情報が作成される。結局、端末装置 10 の利用者が、「日米貿易摩擦」なる作品を再生した場合、甲に対して 20 円、乙に対して 5 円を支払う旨の課金情報が作成されることになり、この課金情報に基づいて、銀行口座を利用した決済を自動的に行うことができる。端末装置 10 の利用者としては、単に、「日米貿易摩擦」という 1 つの作品を鑑賞し、その対価として 25 円支払ったことになり、甲に対して 20 円、乙に対して 5 円という対価の分配先については意識しないですむ。このようなシステムでは、特に、多数箇所の引用を含んだ作品や、入れ子になった多重引用を含んだ作品を鑑賞する場合に、非常に効率的な対価処理が実現できることになる。

【0046】なお、前述したように、各端末装置に特定の作品情報を取り込むためには、ステップ S 3 において、統括管理装置 60 によるアクセス許可が出されることが前提となる。したがって、統括管理装置 60 においては、どの端末装置により、どの作品情報がアクセスされたか、という履歴情報が蓄積されてゆくことになる。このシステムでは、ステップ S 1 における作品リストの提示を行う際に、この履歴情報を利用するようにしている。すなわち、履歴情報は、各ユーザが過去にどのような作品をアクセスしたかという事実を示すものであり、ユーザの趣味、嗜好、生活環境などを把握する上で貴重なデータとなる。そこで、各ユーザに対しては、履歴情報を参考にして、利用度がより高いと思われる作品情報を優先的に知らせるように、作品リストの提示をカスタマイズすることができる。また、前述したように、この履歴情報を種々の商品の販売促進用の情報として利用することも可能である。

【0047】なお、処理演算支援装置 80 は、作品情報保存装置 70 から各端末装置へ作品情報を伝送する処理を支援する機能を有する。既に述べたように、この実施例のシステムでは、エンドユーザ用端末装置 10 として、汎用のパーソナルコンピュータやテレビゲーム装置などの低価格のコンピュータを利用しており、大型コン

コンピュータのような高度な画像処理や演算を実行することはできない。そこで、高度な処理や演算を実行することが必要な素材データについては、作品情報保存装置 7 0 から端末装置 1 0 に直接伝送する代わりに、作品情報保存装置 7 0 から一旦処理演算支援装置 8 0 へ伝送し、ここで必要な処理演算を行い、処理演算後の素材データを端末装置 1 0 に伝送するようにしている。このように、処理演算支援装置 8 0 を仲介して素材データを加工することにより、端末装置 1 0 側での画像処理や演算の負担を軽減させることができる。ステップ S 8 における支援処理は、このような処理演算支援装置 8 0 における処理演算の実行を示すものである。ステップ S 7 は、端末装置 1 0 の機能と、伝送すべき素材データの内容と、を考慮して、このような支援処理が必要か否かを判断するステップであり、この実施例では、統括管理装置 6 0 において判断を行うようにしている。

【0048】このような支援処理としては、たとえば、カラー画像データの変換処理が考えられる。一般にカラー画像と言っても、1画素を32ビットで表現するいわゆる「フルカラー画像」もあるし、これを16ビット、あるいは8ビットで表現するカラー画像もある。そこで、たとえば、作品情報保存装置 7 0 内の素材データが、32ビットのフルカラー画像で用意されていたとしても、端末装置 1 0 側が8ビットのカラー画像にしか対応できないような場合は、32ビットカラー画像を8ビットカラー画像に変換する演算処理が必要になる。また、作品情報保存装置 7 0 内の素材データが高解像度で用意されているのに、端末装置 1 0 側は低解像度にしか対応できないような場合も、高解像度画像データから低解像度画像データへ間引きする処理が必要になる。あるいは、素材データのフォーマットが、端末装置 1 0 で取り扱えるフォーマットと異なる場合には、フォーマット変換処理が必要になる。このような処理を、端末装置 1 0 側に負担させると、リアルタイムでの作品提示に支障を及ぼすことになる。素材データの伝送路上に、高度な演算処理能力をもつ処理演算支援装置 8 0 を介在させてこのような処理を行わせるようにすれば、このような問題はなくなる。

【0049】＜編集者用端末装置による編集処理＞最後に、編集者用端末装置 5 0 における編集手段 5 3 およびデータ保存手段 5 4 の機能について述べておく。図 1 に示す実施例のシステムでは、前述したように、エンドユーザ用端末装置 1 0 を汎用パーソナルコンピュータやテレビゲーム装置により、編集者用端末装置 5 0 を汎用ワークステーションにより、それぞれ構成している。ここで、編集者用端末装置 5 0 は、中小の情報提供会社やマルチメディア作品制作会社に設置することを意図した装置であり、作品提示手段 5 1 および一時記憶手段 5 2 の他に、編集手段 5 3 およびデータ保存手段 5 4 を備えている。

【0050】編集手段 5 3 は、素材データや引用データに基いて、新たな作品を作成し、この新たな作品についての作品情報を、ネットワーク 1 0 0 を介して作品情報保存装置 7 0 に新規保存する処理を行う機能を有し、図 7 に示すハードウェア構成においては、ディスク装置 1 0 7 内にインストールされた「本システムのアプリケーションプログラム」内に組み込まれた編集用ソフトウェアに相当する。

【0051】作品情報保存装置 7 0 内には、種々の素材データが作品情報として登録されており、編集者用端末装置 5 0 の使用者（以下、編集者という）は、編集手段 5 3 を利用して、これらの素材データを自由に組み合わせ、新たな作品を作成することができる。たとえば、図 5 に示すような作品情報をもった作品「日米貿易摩擦」を作成する場合は、編集者は、素材データ A, B, C を自分で用意する。標題ロゴ 1 のような絵柄を作成できる作図ソフトウェアや、本文記事 2 のようなテキストを入力できるワードプロセッサソフトウェアや、グラフ 7 のようなグラフ作成を行うことができるグラフ作成用ソフトウェアを、本システムのアプリケーションプログラムに包含させておけば、編集者はこれらのソフトウェアを用いて素材データ A, B, C を用意することができる。あるいは、別なアプリケーションソフトウェアを用いてこれらの素材データ A, B, C を用意してもかまわない。作品「日米貿易摩擦」では、これらの素材データの他に、引用データ D が必要になる。これは、引用対象となる作品「Mr. K のインタビュー」に付された識別番号を、そのまま引用データ D として用いればよい。編集手段 5 3 には、このように、用いる素材データや引用データを特定し、これらについての作品構成データを作成する編集機能が備わっている。すなわち、編集者が、この編集機能を利用して、個々の素材データを所望の位置に所望の倍率で割り付けると、そのような割り付けを行うための指示が、作品構成データとして生成される。こうして、作品「日米貿易摩擦」が作成できたら、これを新規作品として登録する旨の指示を編集手段 5 3 に与える。このとき、この作品についての財産権データを設定する。すなわち、権利者として自己の名前や識別コードなどを入力し、所望の対価額および利用制限を設定する入力を行えばよい。すると、統括管理装置 6 0 に対して、この新規作品を登録するよう要求が出される。統括管理装置 6 0 は、この新規作品を作品情報保存装置 7 0 内の新たな収容先に割り当て、その収容先を示す情報を作品管理情報に追加する。こうして、図 5 に示すような、素材データ A, B, C、内容リスト、作品構成データ、および財産権データから構成される作品情報が作成できたら、これをネットワーク 1 0 0 を介して作品情報保存装置 7 0 まで伝送し、作品情報保存装置 7 0 内のデータベースに新規登録すればよい。

【0052】このように、作品情報保存装置 7 0 内の作



品情報は、ネットワーク 100 を介して編集者に開放されている。編集者は、この作品情報保存装置 70 内に登録された作品や素材を自由に利用して新たな作品を作成することができ、この作品を登録することができる。また、作品情報保存装置 70 内に用意されている素材だけでなく、独自に用意した新たな素材データを追加して、新たな作品を作成することもできる。編集者によるこのような活動が活発に行われれば、作品情報保存装置 70 内に登録された作品情報は時間とともに増えてゆく。しかも、すべての作品情報は、統括管理装置 60 の管理下においてデータベースとして一元管理されており、相互引用を簡単に行うことができる。すなわち、他の作品を引用する場合には、その作品を特定する引用データを用意するだけですむ。しかも、個々の作品ごとに財産権データが付与されているので、知的財産権に関する管理を各作品、素材ごとに独立して行うことができる。

【0053】一方、データ保存手段 54 は、作品情報保存装置 70 内の作品情報をダウンロードするための手段であり、図 7 に示すハードウェア構成においては、ディスク装置 107 によって構成される手段である。前述したように、本システムにおいて作品の鑑賞（再生）を行う場合、生の素材データは、一時記憶手段 52（図 7 における RAM 106）に一時的に記憶され、再生が終了すると順次消去される。本明細書では、このような、提示のための一時的なデータの取り込み（いわゆる閉鎖系内でのデータ配給）については、ダウンロードという文言を用いずに区別している。このように、ダウンロードを行っていないので、鑑賞後は、生の素材データが端末装置内に残っていないことになる。したがって、ユーザが同じ作品をもう一度鑑賞する場合には、再度対価を支払って（場合によっては割引価格あるいは無償で）、素材データの伝送を受けることになる。一般のエンドユーザにとっては、このような方式でも特に問題は生じない。むしろ、知的財産権の侵害行為を防ぐ上では、このような方式が優れている。素材データが端末装置内に残っていないために、不正利用されるおそれがないためである。

【0054】ところが、編集者用端末装置 50 のユーザである編集者の立場からは、ダウンロードを行って、より自由度の高い編集を行えるようにした方がメリットが大きい。もちろん、本システムでは、ダウンロードを全く行わなくても、新たな作品を作成し、これを作品情報保存装置 70 に新規登録することは可能である。一時記憶手段 52（RAM 106）内に一時的に格納した素材データに対して、編集手段 53（本システムのアプリケーションプログラム内の編集ルーチン）を機能させればよいのである。編集後には、一時記憶手段 52 内の生の素材データは消去されるが、編集によって作成された新たな作品についての作品情報は、作品情報保存装置 70 内に登録されることになる。しかし、このような方式で

は、編集者はあくまでも「本システムのアプリケーションプログラム内の編集ルーチン」を用いた編集しか行うことができず、市販の種々のアプリケーションプログラムを用いた編集はできない。そこで、この実施例では、編集者用端末装置 50 については、生の素材データをデータ保存手段 54（ディスク装置 107）内にダウンロードすることを認めている。編集者は、ダウンロードした素材データに対して、市販の種々のアプリケーションプログラムを用いて加工や編集処理を施し、新たな作品を作成し、これを再び本システムのアプリケーションプログラム（編集手段 53）に引き渡し、作品情報保存装置 70 内に新規登録することが可能になる。また、希望すれば、ダウンロードした素材データを、本システムとは完全に切り離し、CD-ROM などの別の媒体を使って配布したりすることも可能になる。

【0055】ただ、同じ作品を、単に再生して鑑賞する場合と、ダウンロードして利用する場合とでは、利用者の享受する経済的な価値は当然異なる。そこで、財産権データにおいては、作品の利用態様ごとに異なる対価額が設定されている。たとえば、図 6 に示す作品情報では、財産権データの対価額として、「再生利用＝5 円、ダウンロード使用＝500、000 円」という設定がなされている。したがって、この「Mr. K のインタビュー」という作品を再生して鑑賞する場合は、5 円の対価が課金されることになるが、これをダウンロードして利用する場合は、500、000 円の対価が課金されることになる。各端末装置における利用形態が、単なる再生であるのか、ダウンロードであるのか、は統括管理装置 60 において把握されているので、統括管理装置 60 は、利用形態に応じた正しい課金情報を作成することができる。

【0056】また、作者によっては、「自分の作品を引用されたくない」とか、「引用する場合には、このような制限条件を付しておきたい」といったことを要望する場合が少なくない。そこで、本システムでは、財産権データに、利用制限に関する条件を付加してある。個々の作品の利用態様は、この条件によって制限を受けることになる。たとえば、図 6 に示す「Mr. K のインタビュー」なる作品については、「部分引用不可」という利用制限が付加されている。したがって、この作品を引用する場合には、作品ごとそっくり全部を引用しなければならず、素材データ F（略歴 6）をカットして、素材データ E（動画 3）の部分だけを引用するようなことは許されない。また、図 5 に示す「日米貿易摩擦」なる作品については、「ダウンロード不可、素材データ A のみの単独引用不可」という利用制限が付加されている。したがって、この作品は、ダウンロードすることはできない。したがって、編集者用端末装置 50 において、この作品を引用した新たな作品を作成する場合には、一時記憶手段 52 に一時的に格納した素材データに対して編集手段

53を用いた編集を行うことだけが許され、データ保存手段54にダウンロードして市販のアプリケーションソフトウェアによる編集を行うことは許されない。また、素材データA（標題ロゴ1）だけを単独で引用することは禁止されているので、この標題ロゴ1だけを自分の作品に引用するような利用はできないことになる。

【0057】財産権データ内のこのような利用制限情報は、統括管理装置60によって把握されるため、端末装置側において、利用制限に抵触するような操作を行ったとしても、統括管理装置60によってその操作を無効にすることができ、したがって、各作品の知的財産権管理を確実に行うことが可能になる。

【0058】また、財産権データとして、情報仲介料のような項目を設けることもできる。たとえば、利用者甲が、ある作品Aを鑑賞したところ、この作品Aの中で別な作品Bが引用されていたことを認識したとする。そこで、利用者甲が、この作品Bを引用して別な作品Cを新規に作成したものとしよう。この場合、作品Cの中では作品Bが引用されているので、別な利用者乙が、作品Cを鑑賞すれば、作品Cの作者（甲）と作品Bの作者には対価が支払われることになる。ところが、作品Cの作者に、作品Bの存在を紹介したのは作品Aの作者であるから、作品Cの作者（甲）は、作品Cの財産権データとして情報仲介料のような項目を設定しておき、利用者乙が、作品Cを鑑賞した場合には、作品Aの作者にも情報仲介料としての対価が支払われるようにすることもできる。

【0059】以上、本発明を図示する実施例に基いて説明したが、本発明はこの実施例に限定されるものではなく、この他にも種々の態様で実施可能である。たとえば、上述の実施例では、エンドユーザ用端末装置10をパーソナルコンピュータやテレビゲーム装置で、編集者用端末装置50をワークステーションで、それぞれ構成しているが、これらの端末装置を必ずしもこのようなハードウェアで構成する必要はない。また、上述の実施例では、編集手段53およびデータ保存手段54を編集者用端末装置50にのみ用意しているが、エンドユーザ用端末装置10にもこれらの手段を設けるようにしてもかまわない。たとえば、エンドユーザ用端末装置10には、一般のユーザが利用できる程度の簡易な編集機能を設けておき、編集者用端末装置50には、プロフェッショナルが利用するための高度な編集機能を設けておく、という形態も可能である。より具体的には、エンドユーザ用端末装置10に設ける簡易編集機能として、素材データの一部を切り出し、オリジナルな作品構成データを作成し、これを端末装置10内に保存する機能を用意することができる。あるいは、異なる作品情報間において、情報の関連性や相互の参照関係・引用関係を示すリンク情報を付加するような機能を用意することもできる。この場合、このリンク情報を第三者が利用するにあ

たっては、二次的著作物の利用として対価の支払を行うようにすることができる。このような利用形態によれば、システム全体の情報が組織化され、従来のような単独作品を流通させるだけのネットワークでは不可能であった、利用者総員による価値の生長が達成できる。

【0060】なお、編集加工を行った結果得られる新たな作品を、端末装置10や作品情報保存装置70に保存する作業は、統括管理装置60の管理下で行うようにするのが好ましい。こうすることにより、統括管理装置60は、行われた編集加工作業の結果を解析し、その利用態様に応じた利用料金を課金することができる。また、この解析により、各素材データごとの利用者の関心度を測定することができるので（たとえば、ある利用者が特定の素材データに対して編集加工を行ったとすれば、その利用者はその素材データに対して、通常の鑑賞を行う以上の強い関心を示したことになる。）、利用者に別な情報を提示するときの情報の優先度の設定や、通信販売のためのダイレクトマーケティングに応用することができる。

#### 【0061】

【発明の効果】以上のとおり、本発明に係るネットワークを用いた著作物提供システムによれば、素材データ、引用データ、作品構成データ、財産権データ、によって構成した作品情報を作品情報保存装置に收容し、必要に応じて各端末装置に必要な作品を伝送するようにし、伝送された作品についての財産権データに基づいて、個々の作品ごとに知的財産権の管理を行うようにしたため、提供した著作物に付随する知的財産権の管理を効率的に行うことができるようになる。

#### 【図面の簡単な説明】

【図1】本発明の一実施例に係るネットワークを用いた著作物提供システムの基本構成を示すブロック図である。

【図2】図1のシステムにおいて用意されたマルチメディア作品を、ディスプレイ画面上に表示した状態を示す図である。

【図3】図2に示す作品を更に展開した状態を示す図である。

【図4】図1のシステムで用いられる作品情報の一般的な構成を示す図である。

【図5】図2に示す作品についての具体的な作品情報の構成内容を示す図である。

【図6】図5に示す作品情報において引用されている別な作品の作品情報を示す図である。

【図7】図1のシステムにおける端末装置10のハードウェア構成を示すブロック図である。

【図8】図1のシステム全体の動作を説明する流れ図である。

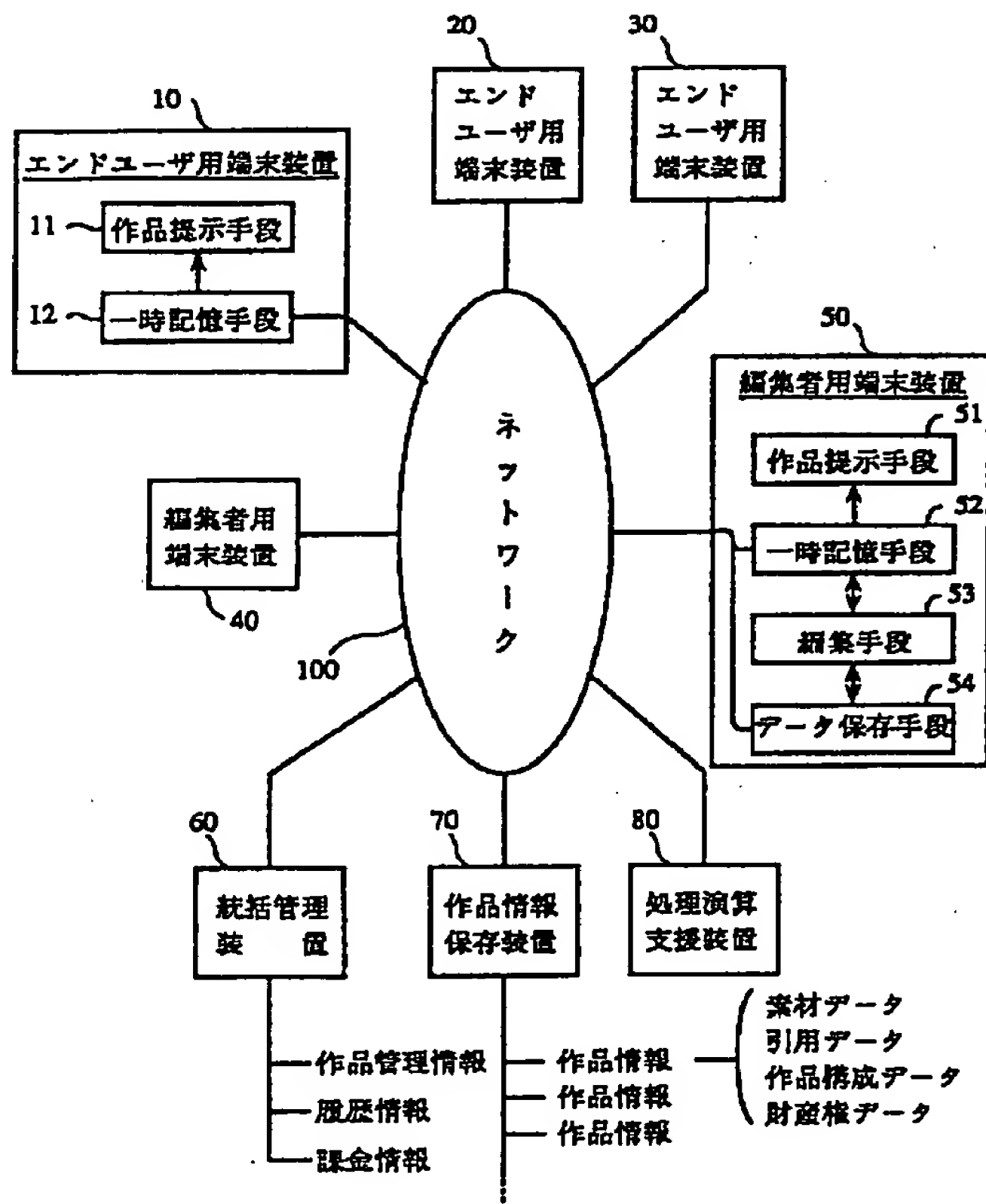
#### 【符号の説明】

1…標題ロゴ

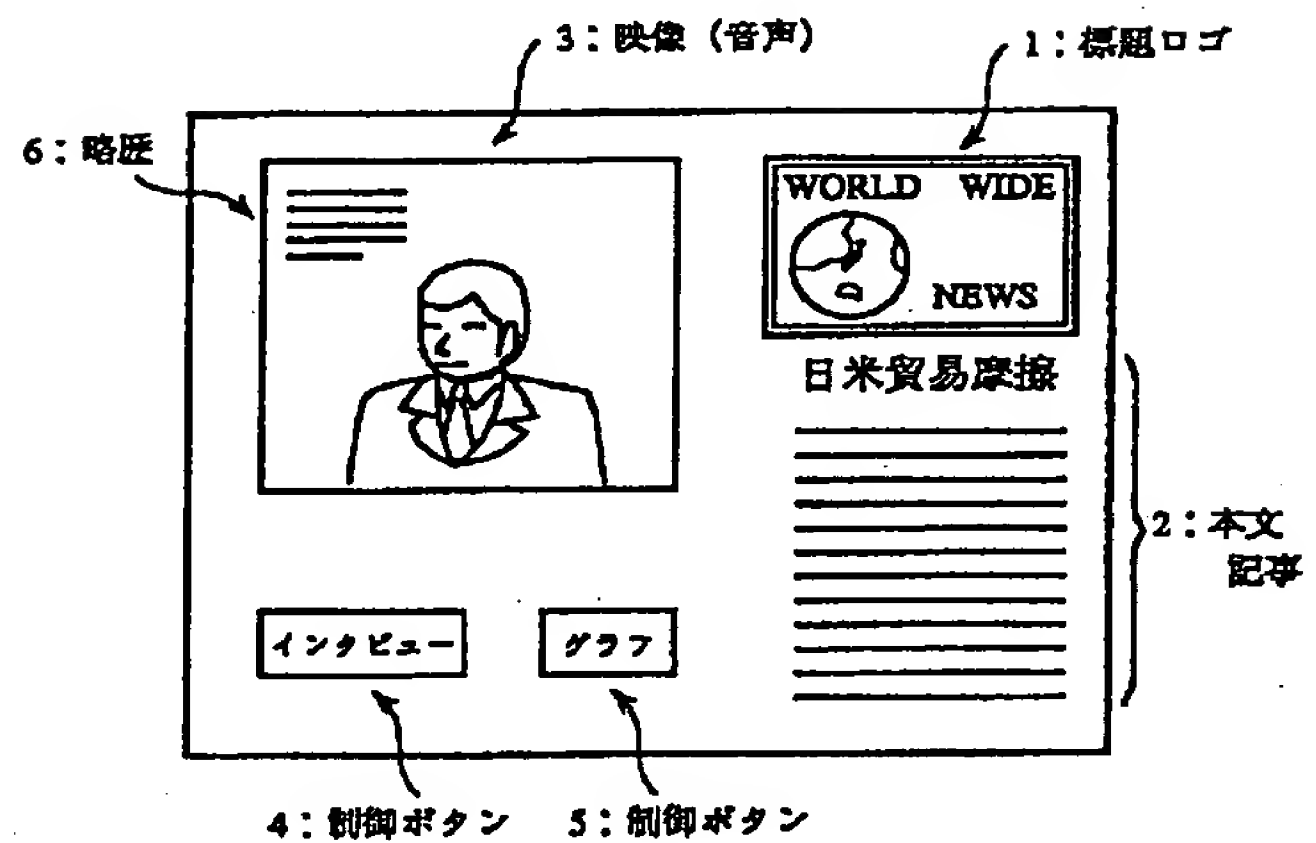
- 2…本文記事  
 3…映像(音声)  
 4, 5…制御ボタン  
 6…略歴  
 7…グラフ  
 8…制御ボタン  
 10, 20, 30…エンドユーザ用端末装置  
 11…作品提示手段  
 12…一時記憶手段  
 40, 50…編集者用端末装置  
 51…作品提示手段  
 52…一時記憶手段  
 53…編集手段  
 54…データ保存手段

- 60…統括管理装置  
 70…作品情報保存装置  
 80…処理演算支援装置  
 100…ネットワーク  
 101…ターミナルアダプタ  
 102…演算処理装置  
 103…ディスプレイ装置  
 104…スピーカ  
 105…ROM  
 106…RAM  
 107…ディスク装置  
 108…キーボード  
 109…マウス

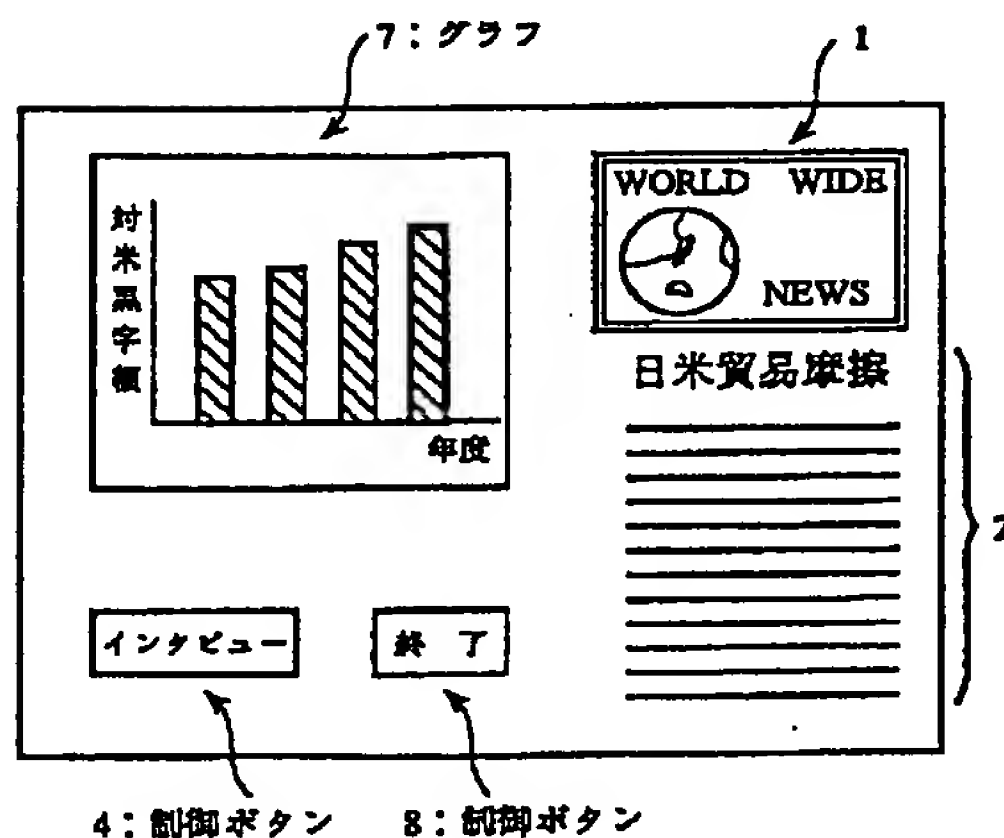
【図1】



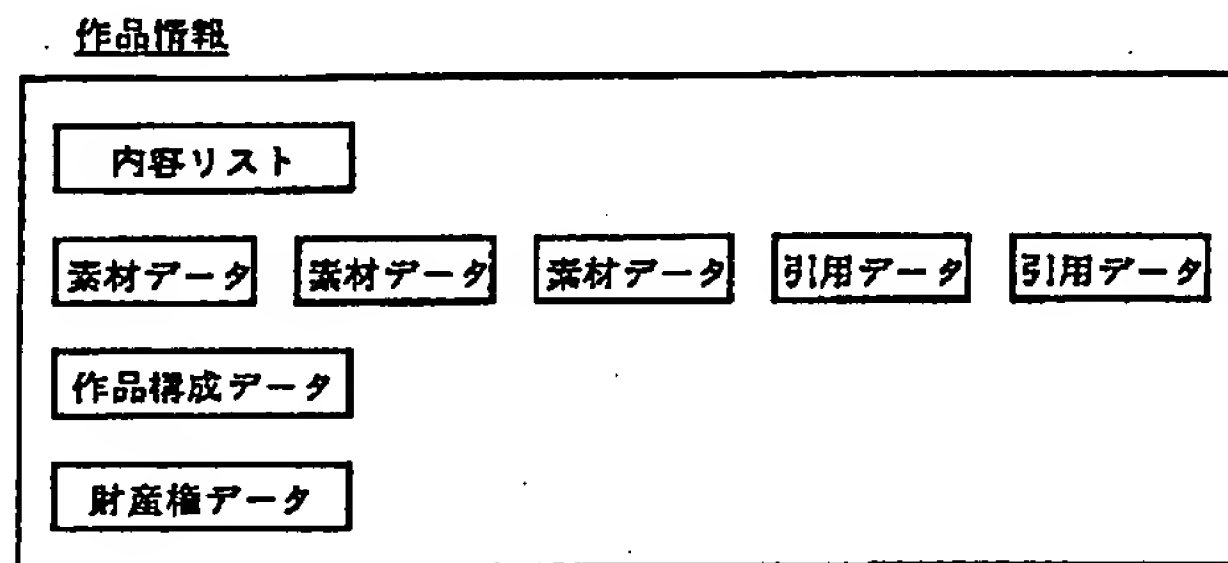
【図2】



【図3】



【図4】



【図5】

## 作品名「日米貿易摩擦」の作品情報

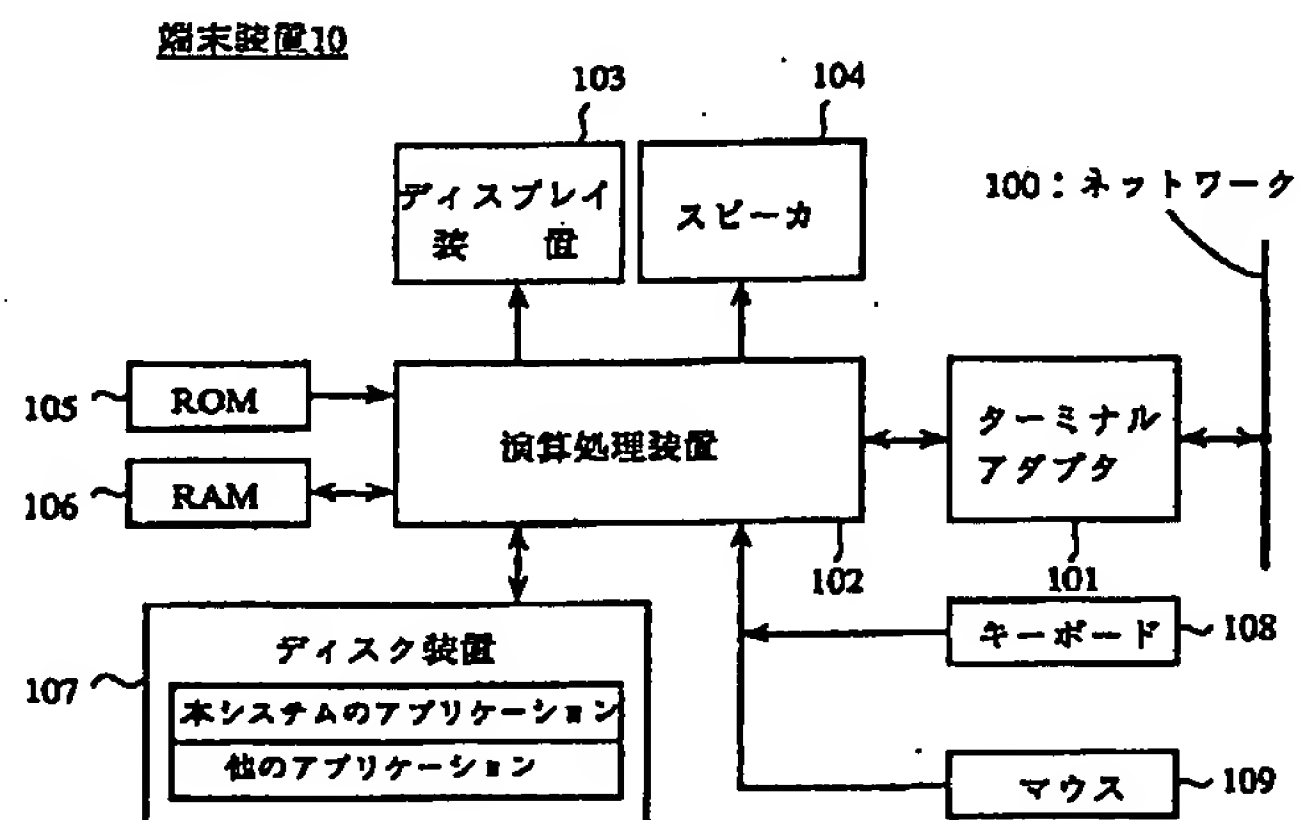
- ① 内容リスト：素材データA, B, C, 引用データD
- ② 素材データA (課題ロゴ1の画像データ)  
素材データB (本文記事2のテキストデータ)  
素材データC (グラフ7の画像データ)  
引用データD (「Mr. Kのインタビュー」を特定するデータ)
- ③ 作品構成データ (作品を構成するための指示)
  - 各素材のレイアウト位置, 倍率
  - 制御ボタン4, 5のパターン, レイアウト位置, 機能
  - 合成手順, 同期指定
- ④ 財産権データ
  - 権利者 : 甲
  - 対価額 : 再生利用=20円
  - 利用制限 : ダウンロード不可, 素材データAのみの単独引用不可

【図6】

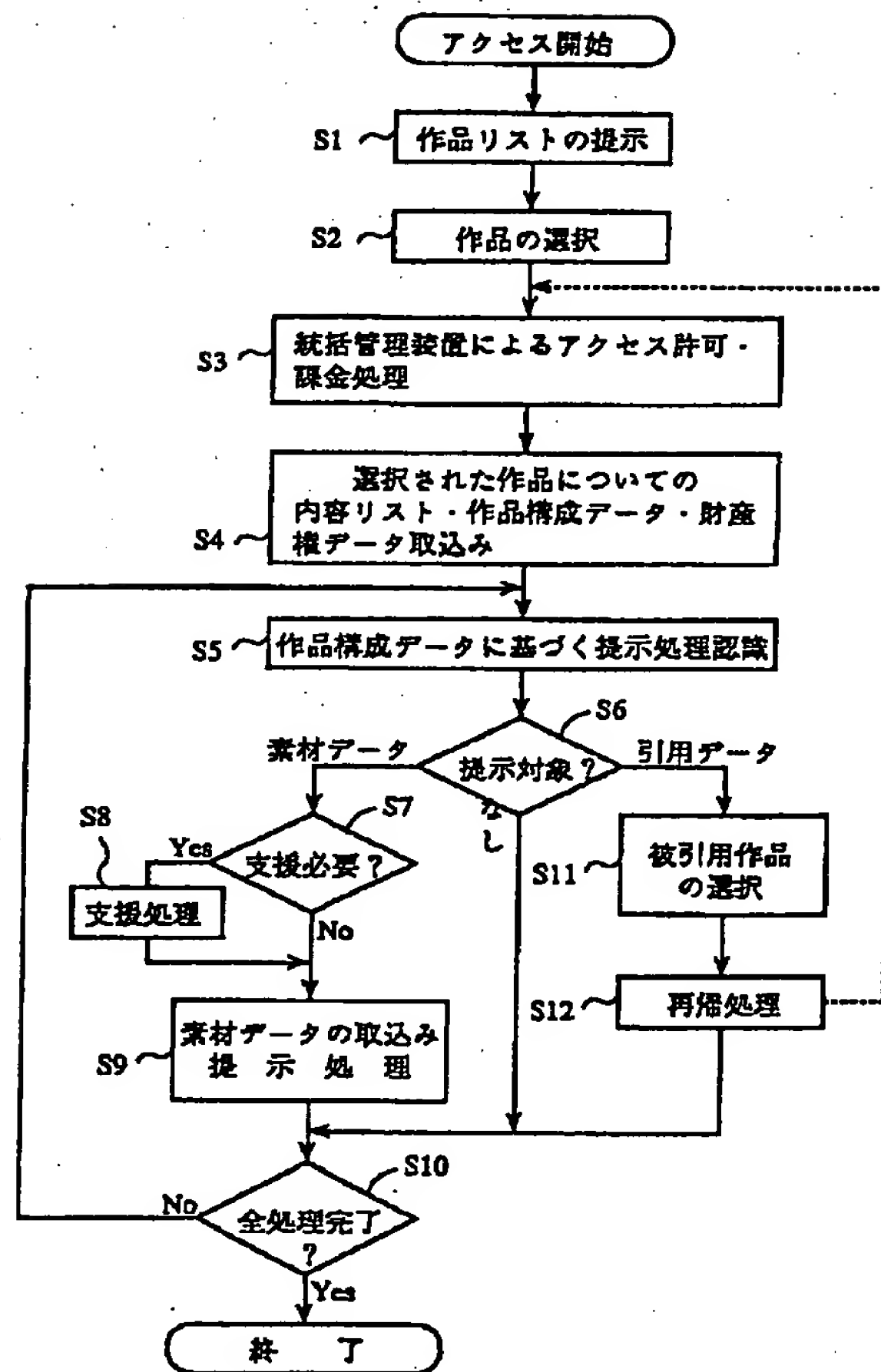
## 作品名「Mr. Kのインタビュー」の作品情報

- ① 内容リスト：素材データE, F
- ② 素材データE (動画3の画像データ)  
素材データF (略歴6のテキストデータ)
- ③ 作品構成データ (作品を構成するための指示)
  - 各素材のレイアウト位置, 倍率
  - 合成手順, 同期指定
- ④ 財産権データ
  - 権利者 : 乙
  - 対価額 : 再生利用=5円, ダウンロード利用=500,000円
  - 利用制限 : 部分引用不可

【図7】



【図 8】



フロントページの続き

(51)Int.C1.<sup>6</sup>

H 0 4 L 12/18

識別記号

庁内整理番号

F I

技術表示箇所

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-185448

(43) 公開日 平成8年(1996)7月16日

(51) Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 17/60				
	15/00	3 9 0	9364-5L	
G 0 9 C 1/00			7259-5J	

G 0 6 F 15/ 21 Z

H 0 4 L 9/ 00 Z

審査請求 未請求 請求項の数48 O L (全 36 頁) 最終頁に続く

(21) 出願番号 特願平7-228368

(22) 出願日 平成7年(1995)9月5日

(31) 優先権主張番号 特願平6-237673

(32) 優先日 平6(1994)9月30日

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願平6-264199

(32) 優先日 平6(1994)10月27日

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願平6-269959

(32) 優先日 平6(1994)11月2日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005979

三菱商事株式会社

東京都千代田区丸の内2丁目6番3号

(72) 発明者 斉藤 誠

東京都千代田区丸の内二丁目6番3号 三  
菱商事株式会社内

(72) 発明者 初木 単一

東京都千代田区丸の内二丁目6番3号 三  
菱商事株式会社内

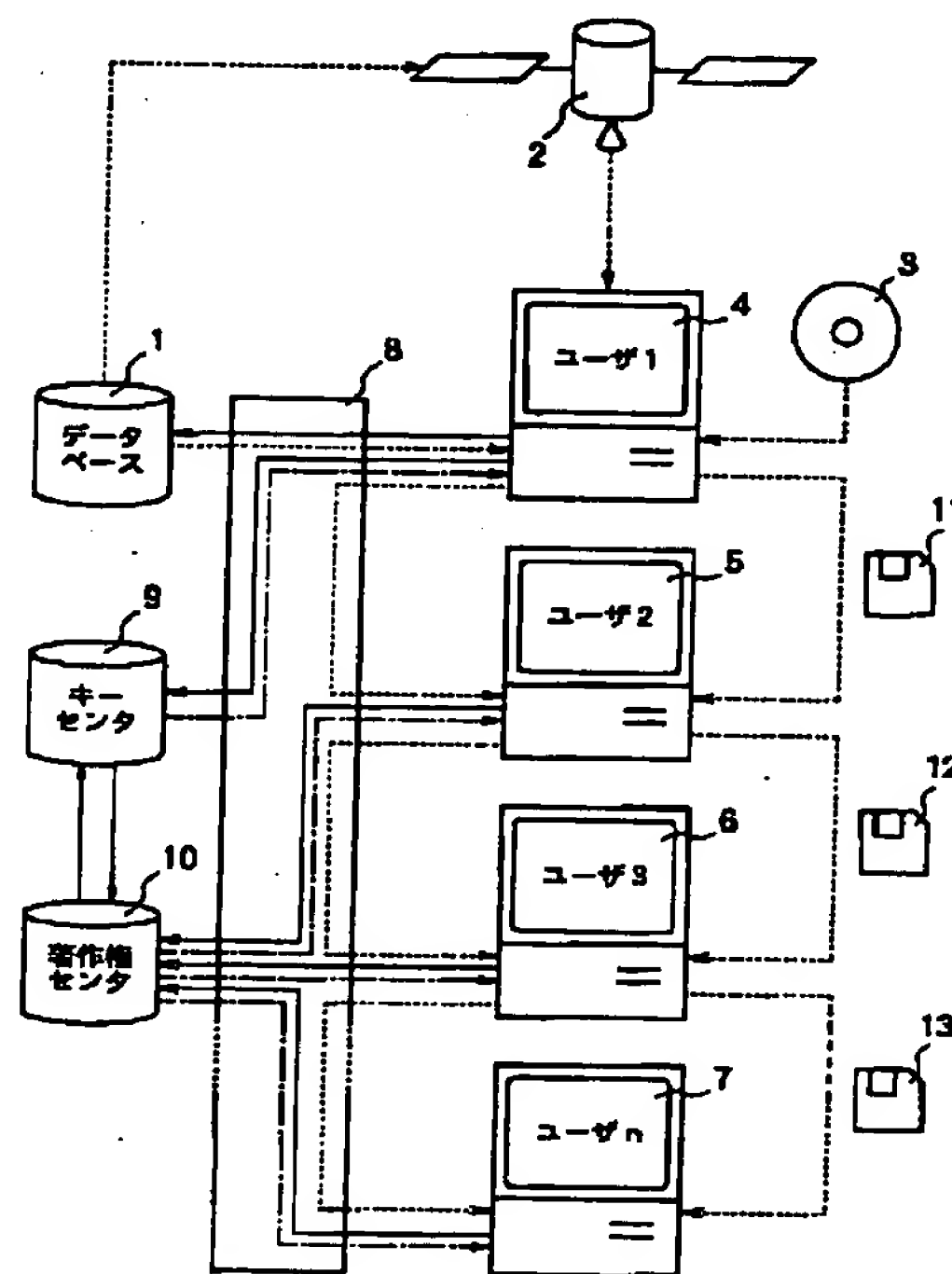
(74) 代理人 弁理士 南條 貞一郎

(54) 【発明の名称】 データ著作権管理システム及びデータ著作権管理装置

(57) 【要約】 (修正有)

【課題】 マルチメディアシステムに於けるデータ著作権、管理システムを提供する。

【解決手段】 データベース1からユーザ4～9に供給されるデータは暗号化して配布され、ユーザは鍵管理センタ9あるいは著作権管理センタ10から入手した暗号鍵を用いて暗号化データを復号化して利用する。ユーザ4～9がデータを保存、複写あるいは転送する場合にデータは再暗号化されるが、この鍵は鍵管理センタ9あるいは著作権管理センタ10から供給されるか著作権管理プログラムによって生成される。





## 【特許請求の範囲】

【請求項1】 暗号化されてデータベースから利用者に供給されるデータの著作権を管理するデータ著作権管理システムであって：該データ著作権管理システムは、データベース1及び鍵管理センタ9を有し；前記暗号化データの復号鍵が前記鍵管理センタ9から前記利用者に供給され；前記利用者が前記データを表示あるいは加工を行う場合には前記復号鍵を用いて前記暗号化データが復号され；前記利用者が前記データあるいは前記加工が行われたデータを保存、複写あるいは転送する場合には前記データが再暗号化される、データ著作権管理システム。

【請求項2】 前記再暗号化に用いられる暗号鍵が前記復号鍵とは異なる暗号鍵である、請求項1記載のデータ著作権管理システム。

【請求項3】 前記著作権管理プログラムが前記利用者が使用する装置のROMに格納されている、請求項3記載のデータ著作権管理システム。

【請求項4】 前記著作権管理プログラムが前記利用者が使用する装置のオペレーティングシステムが管理するシステム領域に格納されている、請求項3記載のデータ著作権管理システム。

【請求項5】 さらに、前記データの著作権を管理する著作権管理プログラムが用いられる、請求項1又は請求項2記載のデータ著作権管理システム。

【請求項6】 さらに、前記データの著作権についての暗号化されていない著作権情報が用いられる、請求項1、請求項2、請求項3、請求項4又は請求項5記載のデータ著作権管理システム。

【請求項7】 前記暗号化されていない著作権情報が著作権情報ラベルとして前記暗号化データに付加されており、前記データの保存、複写あるいは転送が行われた場合に前記著作権情報ラベルが前記データとともに保存、複写あるいは転送される、請求項1、請求項2、請求項3、請求項4、請求項5又は請求項6記載のデータ著作権管理システム。

【請求項8】 前記著作権情報ラベルにデジタル署名がされている、請求項7記載のデータ著作権管理システム。

【請求項9】 データベースから利用者に暗号化されて供給されるデータを利用するためのデータ著作権管理システムであって：前記データ著作権管理システムはデータベース、1鍵管理センタ9及び著作権管理センタ10から構成され；前記データ著作権管理システムでは秘密鍵、利用者情報及び著作権管理プログラムが利用され；前記データベース1はデータを第1秘密鍵によって暗号化して通信ネットワーク8、通信・放送衛星2、記録媒体3を介して1次ユーザ4に配布し；前記1次ユーザ4は前記鍵管理センタ9に対して1次ユーザ情報を提示して利用要求を行い；前記鍵管理センタ9は前記1次

ユーザ情報を前記著作権管理センタ10に転送し；前記鍵管理センタ9は前記第1秘密鍵及び第2秘密鍵とともに著作権管理プログラムを前記通信ネットワーク8を経由して前記1次ユーザ4に転送し；前記1次ユーザ4は前記著作権管理プログラムにより前記第1秘密鍵を用いて前記暗号化データを復号化して利用し；前記復号化データの保存、コピーあるいは転送が行われる場合には前記著作権管理プログラムにより前記第2秘密鍵を用いて再暗号化されるとともにコピーあるいは転送される再暗号化データに暗号化されていない1次ユーザ情報が付加される、データ著作権管理システム。

【請求項10】 前記復号化データがコピーあるいは転送されたときには前記著作権管理プログラムにより前記第1秘密鍵及び第2秘密鍵が廃棄され；前記暗号化データを再利用する前記1次ユーザ4は前記著作権管理センタ10に再暗号化データの再利用のために前記第2秘密鍵の再転送を申し込み；前記第2秘密鍵が再転送される、請求項9記載のデータ著作権管理システム。

【請求項11】 前記第2秘密鍵が再転送されたことにより、前記著作権管理センタ10に前記暗号化データのコピーあるいは転送が登録される、請求項10記載のデータ著作権管理システム。

【請求項12】 2次ユーザ5は前記著作権管理センタ10に前記1次ユーザ情報を提示して利用要求を行い；前記著作権管理センタ10は前記1次ユーザ4に対する前記第2秘密鍵の再転送を確認した上で前記2次ユーザ5に前記第2秘密鍵及び第3秘密鍵及び前記著作権管理プログラムを転送し；前記2次ユーザ5は前記著作権管理プログラムにより前記第2秘密鍵を用いて前記暗号化データを復号化し；前記復号化データの保存、コピーあるいは転送が行われる場合には前記著作権管理プログラムにより前記第3秘密鍵を用いて再暗号化及び再復号化が行われる、請求項10又は請求項11記載のデータ著作権管理システム。

【請求項13】 前記第2秘密鍵が前記著作権管理プログラムにより前記第1秘密鍵、前記ユーザ情報、前記著作権管理プログラムの使用回数のいずれか1つあるいはいくつかに基づいて生成される、請求項9、請求項10、請求項11又は請求項12記載のデータ著作権管理システム。

【請求項14】 データベースから利用者に暗号化されて供給されるデータを利用するためのデータ著作権管理システムであって：前記データ著作権管理システムはデータベース1、鍵管理センタ9及び著作権管理センタ10から構成され；前記データ著作権管理システムでは秘密鍵、利用者情報及び著作権管理プログラムが利用され；1次ユーザ4は前記データベース1に1次ユーザ4情報を提示してデータの利用要求を行い；前記データベース1は要求された前記データを第1秘密鍵を用いて暗号化して前記第1秘密鍵、前記第2秘密鍵及び前記著

著作権管理プログラムとともに前記通信ネットワーク8を経由して前記1次ユーザ4に転送し；前記鍵管理センタ9は前記1次ユーザ情報を前記著作権管理センタ10に転送し；前記鍵管理センタ9は前記第1秘密鍵及び第2秘密鍵とともに著作権管理プログラムを前記通信ネットワーク8を経由して前記1次ユーザ4に転送し；前記1次ユーザ4は前記著作権管理プログラムにより前記第1秘密鍵を用いて前記暗号化データを復号化して利用し；前記復号化データの保存、コピーあるいは転送が行われる場合には前記著作権管理プログラムにより前記第2秘密鍵を用いて再暗号化されるとともにコピーあるいは転送される再暗号化データに暗号化されていない1次ユーザ情報が付加される、データ著作権管理システム。

【請求項15】 前記復号化データがコピーあるいは転送されたときには前記著作権管理プログラムにより前記第1秘密鍵及び第2秘密鍵が廃棄され；前記暗号化データを再利用する場合には前記1次ユーザ4は前記著作権管理センタ10に再暗号化データの再利用のために前記第2秘密鍵の再転送を申し込み；前記第2秘密鍵が再転送される、請求項14記載のデータ著作権管理システム。

【請求項16】 前記第2秘密鍵が再転送されたことにより、前記著作権管理センタ10に前記暗号化データのコピーあるいは転送が登録される、請求項15記載のデータ著作権管理システム。

【請求項17】 前記2次ユーザ5は前記著作権管理センタ10に前記1次ユーザ情報を提示して利用要求を行い；前記著作権管理センタ10は前記1次ユーザ4への前記第2秘密鍵の再転送を確認した上で前記2次ユーザ5に前記第2秘密鍵及び第3秘密鍵及び前記著作権管理プログラムを転送し；前記2次ユーザ5は前記著作権管理プログラムにより前記第2秘密鍵を用いて前記暗号化データを復号化し；前記復号化データの保存、コピーあるいは転送が行われる場合には前記著作権管理プログラムにより前記第3秘密鍵を用いて再暗号化及び再復号化が行われる、請求項15又は請求項16記載のデータ著作権管理システム。

【請求項18】 前記第2秘密鍵が前記著作権管理プログラムにより前記第1秘密鍵、前記ユーザ情報、前記著作権管理プログラムの使用回数のいずれか1つあるいはいくつかに基づいて生成される、請求項14、請求項15、請求項16又は請求項17記載のデータ著作権管理システム。

【請求項19】 データベースから利用者に暗号化されて供給されるデータを利用するためのデータ著作権管理システムであって：前記データ著作権管理システムはデータベース1、鍵管理センタ9及び著作権管理センタ10から構成され；前記データ著作権管理システムでは秘密鍵、公開鍵及び専用鍵が利用され；1次ユーザ4は前記鍵管理センタ9に前記第1公開鍵、第2公開鍵及び1

次ユーザ情報を提示して利用希望データの利用要求を行い；利用要求を受けた前記データベース1は前記データを前記第1秘密鍵を用いて暗号化し、

前記第1秘密鍵を前記第1公開鍵を用いて暗号化し、

前記第2秘密鍵を前記第2公開鍵を用いて暗号化し、

前記暗号化データ、前記暗号化第1秘密鍵及び前記暗号化第2秘密鍵及び著作権管理プログラムを前記1次ユーザ4に転送し；前記1次ユーザ4は著作権管理プログラムにより前記暗号化第1秘密鍵を前記第1専用鍵を用いて復号化し、

前記暗号化データを前記復号化第1秘密鍵を用いて復号化し、

前記暗号化第2秘密鍵を前記第2専用鍵を用いて復号化し、

前記復号化データの保存、コピーあるいは転送が行われる場合には前記著作権管理プログラムにより前記第2秘密鍵を用いて暗号化及び復号化が行われる、データ著作権管理システム。

【請求項20】 前記復号化データがコピーあるいは転送されたときには前記著作権管理プログラムにより前記第1秘密鍵及び第2秘密鍵が廃棄され；前記暗号化データを再利用する前記1次ユーザ4は前記著作権管理センタ10に再暗号化データの再利用のために前記第2秘密鍵の再転送を申し込み；前記第2秘密鍵が再転送される、

請求項19記載のデータ著作権管理システム。

【請求項21】 前記第2秘密鍵が再転送されたことにより、前記著作権管理センタ10に前記暗号化データのコピーあるいは転送が登録される、請求項20記載のデータ著作権管理システム。

【請求項22】 前記2次ユーザ5は前記著作権管理センタ10に前記1次ユーザ情報を提示して利用要求を行い；前記著作権管理センタ10は前記1次ユーザ4に対する前記第2秘密鍵の再転送を確認した上で前記2次ユーザ5に前記第2秘密鍵及び第3秘密鍵及び前記著作権管理プログラムを転送し；前記2次ユーザ5は前記著作権管理プログラムにより前記第2秘密鍵を用いて前記暗号化データを復号化し；前記復号化データの保存、コピーあるいは転送が行われる場合には前記著作権管理プログラムにより前記第3秘密鍵を用いて再暗号化及び再復号化が行われる、請求項20又は請求項21記載のデータ著作権管理システム。

【請求項23】 前記第2秘密鍵が前記著作権管理プログラムにより前記第1秘密鍵、前記ユーザ情報、前記著作権管理プログラムの使用回数のいずれか1つあるいはいくつかに基づいて生成される、請求項19、請求項20、請求項21又は請求項22記載のデータ著作権管理システム。

【請求項24】 各々異なる暗号鍵で暗号化されてデータベース1から利用者に供給される複数のデータを利用

10

20

30

40

50



するためのデータ著作権管理システムであって：該データ著作権管理システムでは暗号鍵、利用者情報及び著作権管理プログラムが利用され；1次ユーザ4は著作権管理センタ10から前記複数の原データ固有の複数の著作権管理プログラム及び複数の第1暗号鍵を入手し、前記複数の原データを前記複数の第1暗号鍵で復号し；前記複数の原データ固有の複数の著作権管理プログラムにより1つ又は複数の第2暗号鍵が生成され；利用された前記複数の原データあるいは複数の加工データは前記複数の原データ固有の複数の著作権管理プログラムにより前記1つ又は複数の第2暗号鍵で暗号化されて加工過程データとともに保存・複写・転送され；前記1つ又は複数の第2の暗号鍵で暗号化された前記複数の原データあるいは前記複数の加工データは2次ユーザ5が前記著作権管理センタ10から入手した前記複数の著作権管理プログラム及び前記1つ又は複数の第2の暗号鍵で復号化されて前記加工過程データを用いて加工されて利用される、データ著作権管理システム。

【請求項25】 前記第2秘密鍵が前記著作権管理プログラムにより前記第1秘密鍵、前記ユーザ情報、前記著作権管理プログラムの使用回数のいずれか1つあるいはいくつかに基づいて生成される、請求項24記載のデータ著作権管理システム。

【請求項26】 データベース1から利用者に暗号化されて供給されるデータを利用するためのデータ著作権管理システムであって：該データ著作権管理システムでは暗号鍵、利用者情報及び著作権管理プログラムが利用され；前記利用者は前記データベース1に利用者情報を提示し；前記データベース1は前記第1利用者に第1暗号鍵で暗号化された前記データを供給し；前記第1利用者は前記著作権管理プログラムを利用して前記第1暗号鍵に基づく第2暗号鍵を生成し；前記第1利用者が前記暗号化データを利用する場合には前記第1暗号鍵を用いて前記暗号化データが復号され；前記第1利用者が前記復号化データを保存、複写あるいは転送する場合には、前記復号化データが前記第2暗号鍵を用いて再暗号化される、データ著作権管理システム。

【請求項27】 前記暗号鍵が秘密鍵である、請求項26記載のデータ著作権管理システム。

【請求項28】 前記暗号鍵が公開鍵及び専用鍵である、請求項26記載のデータ著作権管理システム。

【請求項29】 暗号化されて金融機関から第1利用者に供給されるデジタルキャッシュを利用するためのデジタルキャッシュ管理システムであって：該デジタルキャッシュ管理システムにおいては、前記暗号化デジタルキャッシュデータの復号鍵が金融機関から前記第1利用者に供給され；前記第1利用者が前記デジタルキャッシュデータの確認を行う場合には前記復号鍵を用いて前記暗号化デジタルキャッシュデータが復号され；前記第1利用者が前記復号化デジタルキャッシュ

データを保存する場合、変更されたデジタルキャッシュデータを保存する場合、あるいは第2利用者にデジタルキャッシュデータを転送する場合には前記データが再暗号化される、デジタルキャッシュ管理システム。

【請求項30】 前記再暗号化に用いられる暗号鍵が前記復号鍵とは異なる暗号鍵である、請求項29のデジタルキャッシュ管理システム。

【請求項31】 さらに、前記デジタルキャッシュを管理するデジタルキャッシュ管理プログラムが用いられる、請求項29又は請求項30のデジタルキャッシュ管理システム。

【請求項32】 さらに、暗号化されていない第1利用者情報が用いられる、請求項29、請求項30又は請求項31のデジタルキャッシュ管理システム。

【請求項33】 前記暗号化されていない第1利用者情報が第1利用者情報ラベルとして前記暗号化デジタルキャッシュデータに付加されており、前記デジタルキャッシュデータが保存される場合、変更されたデジタルキャッシュデータが保存される場合、あるいは第2利用者にデジタルキャッシュデータが転送される場合には前記デジタルキャッシュデータとともに保存あるいは転送される、請求項29、請求項30、請求項31又は請求項32のデジタルキャッシュ管理システム。

【請求項34】 前記第1利用者情報ラベルにデジタル署名がされている、請求項33記載のデータ著作権管理システム。

【請求項35】 暗号化されて金融機関から第1利用者に供給されるデジタルキャッシュを利用するためのデジタルキャッシュ管理システムであって：該デジタルキャッシュ管理システムでは暗号鍵、利用者情報及びデジタルキャッシュ管理プログラムが利用され；前記第1利用者は前記金融機関に第1利用者情報を提示し；前記金融機関は前記第1利用者に第1暗号鍵で暗号化された前記デジタルキャッシュを供給し；前記第1利用者は前記デジタルキャッシュ管理プログラムを利用して前記第1暗号鍵に基づく第2暗号鍵を生成し；前記第1利用者が前記暗号化デジタルキャッシュデータの確認を行う場合には前記第1暗号鍵を用いて前記暗号化デジタルキャッシュデータが復号され；前記利用者が前記復号化デジタルキャッシュデータを保存する場合には、前記第2暗号鍵を用いて再暗号化され；前記復号化デジタルキャッシュデータが第2利用者に転送される時に前記第2暗号鍵を用いて再暗号化され、前記再暗号化デジタルキャッシュデータが前記第1利用者情報とともに前記第2利用者に転送され；前記第2利用者から前記金融機関に前記第1利用者情報が提示され；前記金融機関は前記第1利用者情報に基づく前記第2暗号鍵を生成して前記第2利用者に転送し；前記第2利用者は前記転送された第2暗号鍵を用いて前記デジタルキャッシュ管理プログラムにより前記再暗号化デジタルキャ

ッシュデータを復号する、デジタルキャッシュ管理システム。

【請求項36】 前記暗号鍵が秘密鍵である、請求項35のデジタルキャッシュ管理システム。

【請求項37】 前記暗号鍵が公開鍵及び専用鍵である、請求項35のデジタルキャッシュ管理システム。

【請求項38】 暗号化されて金融機関から第1利用者に供給されるデジタルキャッシュを利用するためのデジタルキャッシュ管理システムであって：該デジタルキャッシュ管理システムでは公開鍵及び専用鍵が利用され；前記第1利用者は前記金融機関に第1公開鍵を提示し；前記金融機関は前記第1公開鍵でデジタルキャッシュデータを暗号化して前記第1利用者に供給し；前記第1利用者は前記デジタルキャッシュデータを第1専用鍵を用いて復号し；前記第2利用者は前記第1利用者に第2公開鍵を提示し；前記第1利用者は復号化された前記デジタルキャッシュデータを第2公開鍵で暗号化して第2利用者に転送し；前記第2利用者は前記デジタルキャッシュデータを第2専用鍵を用いて復号する、デジタルキャッシュ管理システム。

【請求項39】 第1利用者から第2利用者に暗号化されて供給されるテレビジョン会議データを利用するためのテレビジョン会議データ管理システムであって：該テレビジョン会議データ管理システムにおいては、前記暗号化テレビジョン会議データの復号鍵が第1利用者から前記第2利用者に供給され；前記第2利用者が前記テレビジョン会議データを利用する場合には前記復号鍵を用いて前記暗号化テレビジョン会議データが復号され；前記第2利用者が前記復号化テレビジョン会議データを保存する場合、加工されたテレビジョン会議データを保存する場合、あるいは第3利用者にテレビジョン会議データを転送する場合には前記データが再暗号化される、テレビジョン会議データ管理システム。

【請求項40】 前記再暗号化に用いられる暗号鍵が前記復号鍵とは異なる暗号鍵である、請求項39のテレビジョン会議データ管理システム。

【請求項41】 さらに、前記テレビジョン会議データを管理するテレビジョン会議データ管理プログラムが用いられる、請求項39又は請求項40のテレビジョン会議データ管理システム。

【請求項42】 さらに、暗号化されていない第2利用者情報が用いられる、請求項39、請求項340は請求項41のテレビジョン会議データ管理システム。

【請求項43】 前記暗号化されていない第2利用者情報が第2利用者情報ラベルとして前記暗号化テレビジョン会議データに付加されており、前記テレビジョン会議データが保存される場合、変更されたテレビジョン会議データが保存される場合、あるいは第2利用者にテレビジョン会議データが転送される場合には前記テレビジョン会議データとともに保存あるいは転送される、請求項

39、請求項40、請求項41又は請求項42のテレビジョン会議データ管理システム。

【請求項44】 前記第1利用者情報ラベルにデジタル署名がされている、請求項43のテレビジョン会議データ管理システム。

【請求項45】 第1利用者から第2利用者に暗号化されて供給されるテレビジョン会議データを利用するためのテレビジョン会議データ管理システムであって：該テレビジョン会議データ管理システムでは暗号鍵、利用者情報及びテレビジョン会議データ管理プログラムが利用され；前記第2利用者は前記第1利用者に第2利用者情報を提示し；前記第1利用者は前記第2利用者に第1暗号鍵で暗号化された前記テレビジョン会議データを供給し；前記第2利用者は前記テレビジョン会議データ管理プログラムを利用して前記第1暗号鍵に基づく第2暗号鍵を生成し；前記第2利用者が前記暗号化テレビジョン会議データを利用する場合には前記第1暗号鍵を用いて前記暗号化テレビジョン会議データが復号され；前記第2利用者が前記復号化テレビジョン会議データを保存、複写あるいは転送する場合には、前記復号化テレビジョン会議データが前記第2暗号鍵を用いて再暗号化される、テレビジョン会議データ管理システム。

【請求項46】 前記暗号鍵が秘密鍵である、請求項45のテレビジョン会議データ管理システム。

【請求項47】 前記暗号鍵が公開鍵及び専用鍵である、請求項45のテレビジョン会議データ管理システム。

【請求項48】 ユーザ端末装置のユーザ端末装置本体のシステムバスに接続して用いられ、マイクロプロセッサ、マイクロプロセッサバスに接続された読み出し専用メモリ、書き込み・読み出しメモリ及び書換可能読み出し専用メモリから構成され、前記読み出し専用メモリには、データベース組織利用ソフトウェア及びユーザデータ等の固定した情報が格納され、

読み出し専用メモリには鍵管理センタあるいは著作権管理センタから供給される第1暗号鍵、第2暗号鍵及び著作権管理プログラムが格納される、データ著作権管理装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明はデジタルデータの利用、保存、複写、加工、転送において著作権を管理するシステムに係るものであり、特にマルチメディアシステムに対して用いることを考慮したものである。

【0002】

【従来の技術】 情報化時代と呼ばれる今日、これまでは各々のコンピュータが独立して保存していた各種のデータを通信回線で各々のコンピュータを接続することによって相互に利用するデータベースシステムが普及しつつ

ある。このデータベースシステムにおいてこれまでに扱われてきた情報は古典的なコンピュータで処理することができる情報量が少ないコード化情報及びせいぜいのところでファクシミリ情報のようなモノクローム2値データであり、自然画及び動画のような情報量が格段に多いデータを取扱うことができなかった。

【0003】ところで、各種電気信号のデジタル処理技術が発展する中で、従来はアナログ信号としてのみ扱われていた2値データ以外の画像信号もデジタル処理技術の開発が進められている。この画像信号のデジタル化によりテレビジョン信号のような画像信号をコンピュータで扱うことが可能となるため、コンピュータが扱う各種のデータと画像信号をデジタル化した画像データとを同時に取り扱う「マルチメディアシステム」が将来の技術として注目されている。

【0004】画像データは、文字データ及び音声データと比較して圧倒的に情報量が多いため、そのままでは保存、転送あるいはコンピュータにおける各種の処理が困難である。そのため、これらの画像データを圧縮／伸張することが考えられ、いくつかの画像データ圧縮／伸張用の規格が作成されてきた。その中で、共通の規格としてこれまでに静止画像用のJ P E G (Joint Photographic image coding Experts Group) 規格、テレビジョン会議用のH. 2 6 1規格、画像蓄積用のM P E G 1 (Moving Picture image coding Experts Group 1) 規格及び現在のテレビジョン放送から高精細度テレビジョン放送に対応するM P E G 2規格が作成された。これらの技術により、デジタル映像データのリアルタイム処理が可能となってきた。

【0005】従来広く普及しているアナログデータは保存、複写、加工、転送をする毎に品質が劣化するため、これらの作業によって生じる著作権の処理は大きな問題とはならなかった。しかし、デジタルデータは保存、複写、加工、転送を繰り返して行っても品質劣化が生じないため、これらの作業によって生じる著作権の処理は大きな問題である。これまで、デジタルデータの著作権処理には的確な方法がなく、著作権法あるいは契約で処理されており、著作権法においてもデジタル方式の録音・録画機器に対する補償金が制度化されているにすぎない。

【0006】データベースの利用法は単にその内容を参照するだけでなく、通常は得たデータを保存、複写、加工することによって有効活用し、加工したデータを通信回線を経由してオンラインであるいは適当な記憶媒体を利用してオンラインで他人に転送したりさらにはデータベースに対して転送し、新しいデータとして登録することさえ可能である。従来のデータベースシステムにおいては文字データのみが対象となっていたが、マルチメディアシステムにおいては、これまでデータベース化されていた文字等のデータに加えて、本来アナログデータで

ある音声データ及び画像データがデジタル化されてデータベースとされる。

【0007】このような状況において、データベース化されたデータの著作権をどのように取扱うかが大きな問題となるが、これまでのところそのための著作権管理手段、特に、複写、加工、転送等の2次利用について完成された著作権管理手段はない。本発明者らは特願平6-46419号及び特開平6-141004号で公衆電話回線を通じて鍵管理センタから利用許可鍵を入手することによって著作権管理を行うシステムを、特開平6-132916号でそのための装置を提案した。

【0008】また、特願平6-64889号において、これらの上記先願発明をさらに発展させることによって、デジタル映像のリアルタイム送信も含むデータベースシステムにおけるデジタルデータの表示（音声化を含む）、保存等の1次利用及び複写、加工、転送等の2次利用における著作権管理方法を提案した。

【0009】この先願のデータベース著作権管理システムは、著作権の管理を行うために、申し込まれた利用形態に対応した利用許可鍵の他に、著作権を管理するためのプログラム、著作権情報あるいは著作権管理メッセージの何れか一つあるいは複数を用いる。

【0010】著作権管理メッセージは申し込みあるいは許可内容に反する利用が行われようとした場合に画面に表示され、ユーザに対して注意あるいは警告を行い、著作権管理プログラムは申し込みあるいは許可内容に反する利用が行われないように監視し管理を行う。

【0011】著作権管理プログラム、著作権情報及び著作権管理メッセージは、各々利用許可鍵とともに全体が供給される場合、データとともに全体が供給される場合及び一部が利用許可鍵とともに供給され、一部がデータとともに供給される場合がある。データ、利用許可鍵、著作権管理メッセージ、著作権情報及び著作権管理プログラムには、暗号化された状態で送信されるが利用時には暗号が解かれる場合、暗号化された状態で送信され表示の際のみに暗号が解かれその他の場合は暗号化された状態である場合、全く暗号化されない場合、の三つの場合がある。

【0012】

【発明の概要】本願においては先願である上記特願平6-64889号において提案されたデータ著作権管理方法を、具体的にしたデータ著作権管理システムを提供する。本発明においては、データ著作権管理システムを原データを保管するデータベース、暗号鍵を管理する鍵管理センタ、データ著作権を管理する著作権管理センタ及びこれらを相互に接続する通信ネットワークから構成し、データベースからユーザに供給されるデータは暗号化して配布され、ユーザは鍵管理センタあるいは著作権管理センタから入手した暗号鍵を用いて暗号化データを復号化して利用する。



【0013】ユーザへのデータ供給は暗号化データを放送等により一方向的に供給する方法と、暗号化データをユーザの要求に応じて双方向的に供給する方法がある。

【0014】データの暗号化に用いられる暗号鍵システムには秘密鍵システム、公開鍵システムあるいは秘密鍵と公開鍵を組み合わせたシステムが採用され、さらにデータ著作権を管理する著作権管理プログラムが採用される。

【0015】ユーザがデータを保存、複写あるいは転送する場合には、鍵が鍵管理センタあるいは著作権管理センタから供給される場合と、著作権管理プログラムによって生成される場合がある。

【0016】また、本発明は単一のデータだけではなく単一のデータベースから供給された複数のデータあるいは複数のデータベースから供給された複数のデータを利用する場合のデータ著作権管理システムにも適用可能である。また、あわせてデータ著作権管理を行うためにユーザ側で使用する装置についても提案する。

【0017】

【実施例】以下、本発明について説明するが初めに暗号技術について一般的な説明をしておく。暗号技術には、秘密鍵暗号方式 (secret-key cryptosystem) と、公開鍵暗号方式 (public-key cryptosystem) がある。秘密鍵暗号方式は、暗号化と復号化に同じ暗号鍵を使用する暗号方式であり、暗号化及び復号化に要する時間が短い反面、秘密鍵が発見され暗号が解読 (Cryptanalyze) されてしまうことがある。一方、公開鍵暗号方式は暗号化用の鍵が公開鍵 (public-key) として公開されており、復号化用の鍵が公開されていない暗号鍵方式であり、暗号化用の鍵は公開鍵と呼ばれ、復号化用の鍵は専用鍵 (private-key) と呼ばれる。この暗号方式を使用するには、情報を発信する側は暗号を受信する側の公開鍵で暗号化 (encryption) し、情報を受信する側は公開されていない専用鍵で復号化 (decryption) する暗号方式であり、暗号化及び復号化に要する時間が長い反面、専用鍵を発見することが殆ど不可能であり暗号の解読が非常に困難である。

【0018】暗号技術においては平文 (plaintext)  $M$  を暗号鍵 (crypton key)  $K$  を用いて暗号化し暗号文 (cryptogram)  $C$  を得る場合を

$$C = E(K, M)$$

と表現し、暗号文  $C$  を暗号鍵  $K$  を用いて復号し平文  $M$  を得る場合を

$$M = D(K, C)$$

と表現する。本発明において使用される暗号方式には、暗号化と復号化に同じ秘密鍵  $K_s$  が使用される秘密鍵方式 (secret-key system) と、平文の暗号化に公開鍵 (public key)  $K_b$  が使用され、暗号文の復号化に専用鍵 (private-key)  $K_v$  が使用される公開鍵方式 (public-key system) が採用される。

【0019】[実施例1] 図1に示されたのは、本願発明に係るデータベース著作権管理システムの第1の実施例であり、この実施例1においては暗号鍵方式として秘密鍵方式が採用される。この図に示す実施例において、1はテキストデータ、コンピュータグラフィックス画面あるいはコンピュータプログラムであるバイナリデータ、デジタル音声データ、デジタル映像データが暗号化された状態で格納されたデータベースであり、2は通信・放送衛星等の人工衛星、3はCD-ROMあるいはフレキシブルディスク等のデータ記録装置、8は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するCATV回線等の通信ネットワーク、4は1次ユーザ端末装置である。また、9は秘密鍵を管理する鍵管理センタ、10はデータベース著作権を管理する著作権管理センタである。

【0020】5、6及び7は各々2次ユーザ端末装置、3次ユーザ端末装置及び $n$ 次ユーザ端末装置であり、11、12及び13は各々フレキシブルディスクあるいはCD-ROM等の記憶媒体である2次ディスク、3次ディスク及び $n$ 次ディスクである。なお、この $n$ は任意の整数であり $n$ が4よりも大きい場合には3次ユーザ端末装置6と $n$ 次ユーザ端末装置7の間及び3次ディスク12と $n$ 次ディスク13との間には対応するユーザ端末装置及びディスクが配置されている。

【0021】これらのうちデータベース1、鍵管理センタ9、著作権管理センタ10、1次ユーザ端末装置4、2次ユーザ端末装置5、3次ユーザ端末装置6及び $n$ 次ユーザ端末装置7は通信ネットワーク8に接続されている。この図において、破線で示された経路は暗号化されたデータの経路であり、実線で示された経路は各ユーザ端末装置からの要求の経路であり、1点鎖線で示された経路は各データベースからの利用形態に対応した許可情報とともに秘密鍵が転送される経路である。また、このシステムを利用する各ユーザは予めデータベース組織に登録をしておく。また、この登録の際にデータベース組織利用ソフトウェアがユーザに対して提供される。このデータベース組織利用ソフトウェアにはデータ通信用プロトコル等の通常の通信用ソフトウェアの他に著作権管理プログラムを動作させるためのプログラムが含まれている。

【0022】データベース1あるいはデータ記録装置3に格納されているテキストデータ、コンピュータグラフィックス画面あるいはコンピュータプログラムであるバイナリデータ、デジタル音声データ、デジタル映像データである原データ $M_0$ が通信ネットワーク8、人工衛星2あるいは記憶媒体3を経由して1次ユーザ端末装置4に一方向的に供給されるが、このときには第1秘密鍵 $K_{s1}$ を用いて暗号化される。

$$C_{m0ks1} = E(K_{s1}, M_0)$$

なお、広告付等の無料で提供されるデータの場合でも著

著作権保護のためには、暗号化を必要とする。

【0023】前に述べた先願である特願平6-64889号には、データの利用形態には、最も基本的な表示の他に保存、加工、コピー、転送があり、利用許可鍵はこれらの利用形態のうちの1つあるいは複数に対応するものが用意され、その管理は著作権管理プログラムによって実行されることが示されている。また、データの表示及び加工のための表示以外の利用形態すなわちデータが保存、コピー、転送される場合には著作権管理プログラムによりデータが再暗号化されることが述べられている。いいかえれば、著作権が主張されたデータは暗号化された状態で流通し、平文化されるのは著作権処理機能を有するユーザ端末装置において、表示あるいは加工のための表示が行われるときのみである。

【0024】この実施例では、これら先願に記載された事項を利用する。供給された暗号化データCm0ks1の1次利用を希望する1次ユーザは鍵管理センタ9に対して1次ユーザ端末装置4を利用し通信ネットワーク8を経由して原データ名あるいは原データ番号等を指定することにより暗号化原データCm0ks1の1次利用申込を行うが、このときに1次ユーザに関する情報Iu1を鍵管理センタ9に提示する。1次ユーザ端末装置4を利用した1次利用申込を受けた鍵管理センタ9は、著作権管理プログラムPとともに1次ユーザがデータベース1から入手した暗号化原データCm0ks1を復号化するための第1秘密鍵Ks1及び復号された原データM0あるいは原データを加工して得られた加工データM1を再暗号化するための第2秘密鍵Ks2を通信ネットワーク8を経由し1次ユーザ端末装置4に転送する。

【0025】復号鍵である第1秘密鍵Ks1、暗号化／復号化鍵である第2秘密鍵Ks2を受け取った1次ユーザ端末装置4において、初めに著作権管理プログラムPを利用して第1秘密鍵Ks1を用いて暗号化原データCm0ks1を復号化し

$$M0 = D(Ks1, Cm0ks1)$$

復号化された原データM0をそのままあるいは加工データM1として利用する。

【0026】原データM0あるいは加工データM1であるデータMが1次ユーザ端末装置4の内部、すなわちメモリあるいは内蔵のハードディスクドライブに保存されている状態ではそのデータを利用することができるのは1次ユーザのみであるが、データMがフレキシブルディスク等の外部記憶媒体11にコピーされた場合、あるいは通信ネットワーク8を経て2次ユーザ端末装置5に転送された場合には、2次利用による著作権の問題が生じる。

【0027】また、1次ユーザが入手した原データM0をそのまま複写して2次ユーザに供給した場合にはその原データM0に何等の改変も加えられていないため、そのデータM0に1次ユーザの著作権は発生しない。しか

し、1次ユーザが入手したデータM0を基に加工を行った場合あるいは他のデータと組み合わせる等の手段を用いることにより新しいデータM1を作成した場合にはそのデータM1に1次ユーザの著作権(2次的著作権 secondarily exploitation right)が発生する。同様に、2次ユーザが1次ユーザから入手した原データM0あるいは加工データM1を基に加工を行った場合あるいは他のデータと組み合わせる等の手段を用いることにより新しいデータM2を作成した場合には、同様に2次ユーザの著作権が発生する。

【0028】この著作権の問題に対処するため、この実施例においてはデータMの保存、コピー、転送が行われるときには著作権管理プログラムPにより第2秘密鍵Ks2を用いてデータMが暗号化され、以後1次ユーザ端末装置4においては第2秘密鍵Ks2を用いてデータMの復号化及び暗号化が行われる。

$$Cmks2 = E(Ks2, M)$$

$$M = D(Ks2, Cmks2)$$

なお、1次ユーザがデータの表示及び加工を行い加工データを得ることは原則として自由にできるが、その場合は著作権管理プログラムによってその回数に制限を設けることができる。

【0029】外部記憶媒体11にデータMがコピーされたとき及び通信ネットワーク8を経てデータが転送されたときには1次ユーザ端末装置4内の第1秘密鍵Ks1及び第2秘密鍵Ks2は著作権管理プログラムPによって廃棄される。したがって、1次ユーザが再度データMを利用する場合には鍵管理センタ9に利用申込を行い、第2秘密鍵Ks2の再交付を受ける必要がある。この第2秘密鍵Ks2の再交付を受けたことは、データMが外部記憶媒体11へコピーあるいは通信ネットワーク8を経由しての2次ユーザ端末装置5へ転送されることによる2次利用が行われたことを意味するから、このことが鍵管理センタ9から著作権管理センタ10に登録され、以後の2次利用が可能になる。

【0030】1次ユーザ端末装置4からの2次ユーザ端末装置5へのデータMの移動は外部記憶媒体11によってあるいは通信ネットワーク8により行われ、外部記憶媒体11へのコピーあるいは通信ネットワーク8を経由して移動が行われるときには、第2秘密鍵Ks2を用いてデータMが暗号化される。

【0031】外部記憶媒体11にデータMがコピーされたとき及び通信ネットワーク8を経てデータMが転送されたときに1次ユーザ端末装置4内の第1秘密鍵Ks1及び第2秘密鍵Ks2は廃棄されるが、このときに1次ユーザ端末装置4内に保存されている暗号化データCmks2に、暗号化されていない1次ユーザ情報Iu1が付加され、暗号化データCmks2を2次ユーザに転送する際に1次ユーザ情報Iu1も転送される。

【0032】1次ユーザからコピーあるいは転送された

暗号化データCmks2の2次利用を希望する2次ユーザは、2次ユーザ端末装置5を利用して通信ネットワーク8を経由して著作権管理センタ10に対して原データ名あるいは原データ番号を指定するとともに2次ユーザ情報Iu2を提示して2次利用申込を行うが、そのときに1次ユーザとの関係を明確にするために暗号化データCmks2に付加されている暗号化されていない1次ユーザ情報Iu1も提示する。著作権管理センタ10は、提示された1次ユーザ情報Iu1に基づきその1次ユーザがそのデータを2次利用するために第2秘密鍵Ks2の再交付を受けていることを確認し、復号化鍵である第2秘密鍵Ks2、暗号化／復号化鍵である第3秘密鍵Ks3を通信ネットワーク8を経由して2次ユーザ端末装置5に転送する。第2秘密鍵Ks2、第3秘密鍵Ks3を受け取った2次ユーザ端末装置5において、著作権管理プログラムPにより第2秘密鍵Ks2を用いて暗号化データCmks2が復号化され

$M = D(Ks2, Cmks2)$   
表示あるいは加工の2次利用が行われる。

【0033】この実施例においては、1次利用申込は鍵管理センタ9が処理し、2次利用申込は著作権管理センタ10が処理する。また、1次ユーザが供給されるデータMは第1秘密鍵Ks1を用いて暗号化されているが、2次ユーザが供給されるデータMは第2秘密鍵Ks2を用いて暗号化されている。一方、1次ユーザに対して鍵管理センタ9からは暗号鍵として第1秘密鍵Ks1及び第2秘密鍵Ks2が転送される。そのため、2次ユーザが1次ユーザであると偽って鍵管理センタ9に対して1次利用申込を行った場合には復号化鍵として第1秘密鍵Ks1が、暗号化／復号化鍵として第2秘密鍵Ks2が転送される。しかし、復号化鍵として転送された第1秘密鍵Ks1を用いて暗号化データCmks2を復号することはできない。したがって、データの利用について虚偽の申込を行うことは不可能であり、その結果データの著作権だけでなく、データについての1次ユーザの著作権も保護される。

【0034】2次ユーザ端末装置5においてデータMの表示及び加工のための表示以外の利用形態である保存、コピー、転送が行われるときには著作権管理プログラムPによって第3秘密鍵Ks3を用いてデータMの暗号化が行われ、以後第3秘密鍵Ks3を用いてデータの復号及び

$Cmks3 = E(Ks3, M)$

$M = D(Ks3, Cmks3)$

なお、2次ユーザが表示及び加工を行い加工データM2を得ることも原則として自由にできるが、その場合は著作権管理プログラムPによってその回数に制限を設けることができる。

【0035】外部記憶媒体12にデータMがコピーされたとき及び通信ネットワーク8を経てデータが転送されたときには2次ユーザ端末装置5内の第2秘密鍵Ks2及

び第3秘密鍵Ks3は著作権管理プログラムPによって廃棄される。したがって、2次ユーザが再度データMを利用する場合には著作権管理センタ10に利用申込を行い、第3秘密鍵Ks3の再交付を受ける必要がある。この第3秘密鍵Ks3の再交付を受けたことは、データMが外部記憶媒体12へコピーあるいは通信ネットワーク8を経由しての3次ユーザ端末装置6へ転送されることによる2次利用が行われたことを意味するから、このことが著作権管理センタ10に登録され、以後の利用が可能になる。

【0036】2次ユーザ端末装置5からの3次ユーザ端末装置6へのデータMの移動は外部記憶媒体12によってあるいは通信ネットワーク8により行われ、外部記憶媒体12へのコピーあるいは通信ネットワーク8を経由して移動が行われるときには、第3秘密鍵Ks3を用いてデータMが暗号化される。

【0037】外部記憶媒体12にデータMがコピーされたとき及び通信ネットワーク8を経てデータMが3次ユーザ端末装置6に転送されたときに2次ユーザ端末装置5内の第2秘密鍵Ks2及び第3秘密鍵Ks3は廃棄されるが、このときに2次ユーザ端末装置5内に保存されている暗号化データCmks3に、暗号化されていない2次ユーザ情報Iu2が付加される、暗号化データCmks3を3次ユーザに転送する際に2次ユーザ情報Iu2も転送される。この場合、各ユーザ情報のデータへの付加は、全てのユーザ情報がコピーあるいは転送の度にデータに付加される場合と、その度に最新のものに書き換えられる履歴が著作権管理センタに保管される場合がある。

【0038】2次ユーザからコピーあるいは転送された暗号化データCmks3の3次利用を希望する3次ユーザは、3次ユーザ端末装置6を利用して通信ネットワーク8を経由して著作権管理センタ10に対して原データ名あるいは原データ番号を指定するとともに3次ユーザ情報Iu3を提示して3次利用申込を行うが、そのときに2次ユーザとの関係を明確にするために暗号化データCmks3に付加されている暗号化されていない2次ユーザ情報Iu2も提示する。著作権管理センタ10は、提示された2次ユーザ情報Iu2に基づきその2次ユーザがそのデータを3次利用するための準備手続き、すなわち第3秘密鍵Ks3の再交付を受けていることを確認し、復号化鍵である第3秘密鍵Ks3、暗号化／復号化鍵である第4秘密鍵Ks4を通信ネットワーク8を経由して3次ユーザ端末装置6に転送する。第3秘密鍵Ks3、第4秘密鍵Ks4を受け取った3次ユーザ端末装置6において、著作権管理プログラムPにより第3秘密鍵Ks3を用いて暗号化データCmks3が復号化され

$M = D(Ks3, Cmks3)$

表示あるいは加工の3次利用が行われる。

【0039】この実施例においては、1次ユーザが供給されるデータMは第1秘密鍵Ks1を用いて暗号化され、



2次ユーザが供給されるデータMは第2秘密鍵Ks2を用いて暗号化されているが、3次ユーザが供給されるデータMは第3秘密鍵Ks3を用いて暗号化されている。そのため、3次ユーザが1次ユーザであると偽って鍵管理センタ9に対して1次利用申込を行った場合には復号化鍵として第1秘密鍵Ks1が、暗号化/復号化鍵として第2秘密鍵Ks2が転送される。しかし、復号化鍵として転送された第1秘密鍵Ks1を用いて暗号化データCmks3を復号化することはできない。また、3次ユーザが2次ユーザであると偽って著作権管理センタ9に対して2次利用申込を行った場合には復号化鍵として第2秘密鍵Ks2が、暗号化/復号化鍵として第3秘密鍵Ks3が転送される。しかし、復号化鍵として転送された第2秘密鍵Ks2を用いて暗号化Cmks3を復号することはできない。したがって、データの利用について虚偽の申込を行うことは不可能であり、その結果データの著作権だけでなく、データについての1次ユーザの著作権及び2次ユーザの著作権も保護される。以下、同様の手続きが4次以降の利用にも適用される。

【0040】以上説明した実施例におけるデータベース1、鍵管理センタ9、著作権管理センタ10は別個に設置されているが、これらは必ずしも別個のものである必要はなく、これらの全てあるいは適当な2つを一体に設置することも可能である。また、1次ユーザからの2次暗号鍵再交付申込は実施例のように鍵管理センタ9に対して行うのではなく著作権管理センタ10に対して行うようにしてもよい。

【0041】[実施例2]次に、実施例2について説明するが、この実施例の大部分の構成は実施例1の構成と同様であるが、著作権管理プログラム、場合によってはさらに第1秘密鍵と第2秘密鍵が、暗号化されて供給される。この実施例でも第1実施例と同様に原データは単一のデータベースから暗号化されて一方向的に供給され、ユーザは供給された原データから必要なものを選択して利用する。なお、実施例2で用いるシステム構成は図1に示された実施例1のシステム構成と異なる点はないため、システム構成についての説明は省略する。

【0042】この実施例において、データベース1に格納されている原データM0が人工衛星2、記憶媒体3あるいは通信ネットワーク8を経由して1次ユーザ端末装置4に一方向的に供給されるが、そのときには第1秘密鍵Ks1を用いて暗号化される。

$$Cm0ks1 = E(Ks1, M0)$$

【0043】供給された暗号化データCm0ks1の1次利用を希望する1次ユーザは鍵管理センタ9に対して1次ユーザ端末装置4を利用し通信ネットワーク8を経由して原データ名あるいは原データ番号等を指定することにより暗号化原データCm0ks1の1次利用申込を行うが、このときに1次ユーザ情報Iu1を鍵管理センタ9に提示する。

【0044】暗号化原データCm0ks1の1次利用申込を受けた鍵管理センタ9は、1次ユーザ情報Iu1を利用して1次ユーザ専用の秘密鍵Ksulを生成し著作権管理センタ10に転送する。

【0045】1次ユーザ専用の秘密鍵Ksulを受け取った著作権管理センタ10は、この1次ユーザ専用秘密鍵Ksulを用いて著作権管理プログラムPを暗号化し、

$$Cpksul = E(Ksul, P)$$

暗号化著作権管理プログラムCpksulを鍵管理センタ9に転送する。このようにして生成された暗号化著作権管理プログラムCpksulは1次ユーザに固有のものである。また、鍵管理センタ9は著作権管理センタ10から受け取った暗号化著作権管理プログラムCpksulとともに復号化鍵である第1秘密鍵Ks1及び復号化/暗号化鍵である第2秘密鍵Ks2を通信ネットワーク8を経由し1次ユーザ端末装置4に転送する。

【0046】暗号化著作権管理プログラムCpksul、第1秘密鍵Ks1、第2秘密鍵Ks2を受け取った1次ユーザ端末装置4において、初めに予め配布されているデータベース組織用ソフトウェアSが1次ユーザ情報Iu1に基づいて1次ユーザ専用秘密鍵Ksulを生成し、

$$Ksul = S(Iu1)$$

生成された1次ユーザ専用秘密鍵Ksulを用いて暗号化著作権管理プログラムCpsulを復号化し、

$$P = D(Ksul, Cpksul)$$

復号化された著作権管理プログラムPを利用して第1秘密鍵Ks1を用いて暗号化原データCm0ks1を復号化し

$$M0 = D(Ks1, Cm0ks1)$$

復号化された原データM0をそのままあるいは加工データM1として利用する。

【0047】原データM0あるいは加工データM1であるデータMの保存、コピー、転送が行われるときには著作権管理プログラムPにより第2秘密鍵Ks2を用いてデータMが暗号化され、以後1次ユーザ端末装置4においては第2秘密鍵Ks2を用いてデータMの復号化及び暗号化が行われる。

$$Cmks2 = E(Ks2, M)$$

$$M = D(Ks2, Cmks2)$$

【0048】外部記憶媒体11にデータMがコピーされたとき及び通信ネットワーク8を経てデータが転送されたときには1次ユーザ端末装置4内の第1秘密鍵Ks1及び第2秘密鍵Ks2は著作権管理プログラムPによって廃棄される。したがって、1次ユーザが再度データMを利用する場合には鍵管理センタ9に利用申込を行い、第2秘密鍵Ks2の再交付を受ける必要がある。この第2秘密鍵Ks2の再交付を受けたことは、データMが外部記憶媒体11へコピーあるいは通信ネットワーク8を経由しての2次ユーザ端末装置5へ転送されることによる2次利用が行われたことを意味するから、このことが鍵管理センタ9から著作権管理センタ10に登録され、以後の2

次利用が可能になる。

【0049】1次ユーザ端末装置4からの2次ユーザ端末装置5へのデータMの移動は外部記憶媒体11によってあるいは通信ネットワーク8により行われる。データMの外部記憶媒体11へのコピーあるいは通信ネットワーク8を経由して転送が行われるときには、第2秘密鍵Ks2を用いてデータMが暗号化される。

【0050】外部記憶媒体11にデータMがコピーされたとき及び通信ネットワーク8を経てデータMが転送されたときに1次ユーザ端末装置4内の第1秘密鍵Ks1及び第2秘密鍵Ks2は廃棄されるが、このときに1次ユーザ端末装置4内に保存されている暗号化データCmks2に、1次ユーザについての暗号化されていない情報Iu1が付加される。そのため、暗号化データCmks2を2次ユーザに転送する際に1次ユーザ情報Iu1も転送される。

【0051】1次ユーザからコピーあるいは転送された暗号化データCmks2の2次利用を希望する2次ユーザは、2次ユーザ端末装置5を利用して通信ネットワーク8を経由して著作権管理センタ10に対して原データ名あるいは原データ番号を指定するとともに2次ユーザ情報Iu2を提示して2次利用申込を行うが、そのときに1次ユーザとの関係を明確にするために暗号化データCmks2に付加されている暗号化されていない1次ユーザ情報Iu1も提示する。著作権管理センタ10は、提示された1次ユーザ情報Iu1に基づきその1次ユーザがそのデータを2次利用するために第2秘密鍵Ks2の再交付を受けていることを確認し、提示された2次ユーザ情報Iu2に基づいて2次ユーザ専用の秘密鍵Ksu2を生成する。

【0052】著作権管理センタ10はこの2次ユーザ専用秘密鍵Ksu2を用いて著作権管理プログラムPを暗号化し、

$$Cpksu2 = E(Ksu2, P)$$

暗号化著作権管理プログラムCpksu2、復号化鍵である第2秘密鍵Ks2、暗号化／復号化鍵である第3秘密鍵Ks3を通信ネットワーク8を経由して2次ユーザ端末装置5に転送する。なお、この暗号化著作権管理プログラムCpksu2に1次ユーザに関する情報Iu1を付加しておいてもよい。

【0053】第2秘密鍵Ks2、第3秘密鍵Ks3を受け取った2次ユーザ端末装置5において、データベース組織利用ソフトウェアが2次ユーザ情報Iu2に基づいて2次ユーザ専用秘密鍵Ksu2を生成し、

$$Ksu2 = S(Iu2)$$

生成された2次ユーザ専用秘密鍵Ksu2を用いて暗号化著作権管理プログラムCpsu2を復号化し、

$$P = D(Ksu2, Cpsu2)$$

復号化された著作権管理プログラムPを利用して第2秘密鍵Ks2を用いて暗号化原データCmks2を復号化し

$$M = D(Ks2, Cmks2)$$

復号化されたデータMをそのままあるいは加工して利用

する。

【0054】このように、利用申込を行ったユーザのユーザ情報に基づいてユーザ専用暗号鍵を生成し、生成されたユーザ専用暗号鍵を用いて著作権管理プログラムを暗号化することにより、データ著作権管理システムの安全性が高くなる。また、このときにユーザに供給される各秘密鍵もユーザ専用暗号鍵を用いて暗号化すれば、データ著作権管理システムの安全性がより高くすることができる。

【0055】〔実施例3〕さらに、図1に示されたシステムにおいて、外部記憶媒体11にデータMがコピーされた場合、あるいは通信ネットワーク8を経てデータMが転送された場合に生じる著作権の問題に対応するためのさらに別の方法として、1次ユーザ端末4の使用が行う1次利用申込を表示許可、保存許可及び加工許可だけに限定しそれ以外の利用申込すなわちコピー許可及び転送許可を受けることはできず、コピー許可及び転送許可の申込は別に行うようにし、外部記憶媒体11にデータMがコピーされたとき及び通信ネットワーク8を経てデータが2次ユーザ端末装置5に転送されたときに、1次ユーザ端末装置4内の第1秘密鍵Ks1及び第2秘密鍵Ks2は廃棄されるようにすることもできる。このようにすれば、データMのコピーあるいは転送をより確実に著作権管理センタ10で把握することができる。

【0056】〔実施例4〕図2に示されたのは、本願発明に係るデータ著作権管理システムの実施例4の構成である。図1に示されたシステムでは、暗号化データが衛星2、記録媒体3あるいは通信ネットワーク8を経由して一方的に供給されるが、実施例2では1次ユーザ4からの要求に応じて暗号化データが双方向的に供給される。また、この実施例においては、暗号鍵方式として公開鍵方式が採用される。なお、実施例2がデータ供給手段としてデータベース以外に広告付き等の無料の暗号化する必要の無い衛星放送、地上波放送、CATV放送あるいは記録媒体を用いる場合にも適用可能なことは勿論のことである。

【0057】図1に示されたシステムと同様にこの図に示されたシステムにおいて、1はデータベース、4は1次ユーザ端末装置、5は2次ユーザ端末装置、6は3次ユーザ端末装置、7はn次ユーザ端末装置である。また、14は2次著作権管理センタ、15は3次著作権管理センタ、16はn次著作権管理センタ、8は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するCATV回線等の通信ネットワークである。

【0058】これらのうち、データベース1、1次ユーザ端末装置4、2次ユーザ端末装置5、3次ユーザ端末装置6、n次ユーザ端末装置7、2次著作権管理センタ14、3次著作権管理センタ15、n次著作権管理センタ16は通信ネットワーク8に接続されており相互に接



続可能である。この図において、破線で示された経路は暗号化されたデータの経路であり、実線で示された経路は各ユーザ端末装置からの要求の経路であり、1点鎖線で示された経路は各データベースからの利用形態に対応した許可情報とともに暗号鍵が転送される経路であり、2点鎖線で示された経路はデータベースあるいは各著作権管理センタデータベースから次位の著作権管理センタデータベースへ著作権情報が転送される経路である。また、このシステムを利用する各ユーザは予めデータベース組織に登録をしておく。また、この登録の際にデータベース組織利用ソフトウェアがユーザに対して提供される。このデータベース組織利用ソフトウェアにはデータ通信用プロトコル等の通常の通信用ソフトウェアの他に暗号化された著作権管理プログラムを復号化するためのプログラムが含まれている。

【0059】データベース1を利用するに当たり、1次ユーザは1次ユーザ認証データAu1、第1公開鍵Kb1及び第1公開鍵Kb1に対応する第1専用鍵Kv1、第2公開鍵Kb2及び第2公開鍵Kb2に対応する第2専用鍵Kv2を用意し、1次ユーザ端末装置4を利用し通信ネットワーク8を経由してデータベース1にアクセスする。

【0060】1次ユーザから1次ユーザ認証データAu1、第1公開鍵Kb1、第2公開鍵Kb2の転送を受けたデータベース1は、1次ユーザ認証データAu1を確認し、確認された1次ユーザ認証データAu1を1次ユーザ情報Iu1として2次著作権管理センタ14に転送する。

【0061】一方、データベース1は2個の秘密鍵すなわち第1の秘密鍵Ks1と第2の秘密鍵Ks2を用意する。この2個の秘密鍵の用意は図1に示された実施例1の鍵センタ9を利用して行ってもよい。用意された第1の秘密鍵Ks1及び第2の秘密鍵Ks2中、第2の秘密鍵Ks2も予め著作権管理センタ14に転送される。

【0062】これらの転送が行われた結果著作権管理センタ14には1次ユーザ情報Iu1、原著作権情報Ic及び第2秘密鍵Ks2が格納される。なお、これらの中で原著作権情報Icは著作権使用料分配に用いられる。

【0063】データの利用を希望する1次ユーザは、1次ユーザ端末装置4を利用してデータベース1にアクセスすると、データメニューが転送される。このときデータメニューとともに料金の情報を表示してもよい。

【0064】データメニューが転送されると1次ユーザはデータメニュー検索を行いデータMを選択する。このとき、選択されたデータMの原著作権情報Icが著作権管理センタ14に転送される。

【0065】1次ユーザの要求に応じてデータベース1から原データM0が読み出される。読み出された原データM0は第1秘密鍵Ks1で暗号化される。

$$Cm0ks1 = E(Ks1, M0)$$

この暗号化データCm0ks1には暗号化されていない原著作権者情報Icが付けられている。また、第1の秘密鍵

Ks1を第1の公開鍵Kb1で、第2の秘密鍵Ks2を同じく第2の公開鍵Kb2で暗号化する。

$$Cks1kb1 = E(Kb1, Ks1)$$

$$Cks2kb2 = E(Kb2, Ks2)$$

併せて著作権管理プログラムPも第2の秘密鍵Ks2で暗号化されるが、

$$Cpks2 = E(Ks2, P)$$

著作権管理プログラムPの暗号化は第2の秘密鍵Ks2で暗号化されなければならないものではなく、他の適当な暗号鍵を用いて暗号化することができる。暗号化原データCm0ks1、暗号化著作権管理プログラムCpks2及び2個の暗号化秘密鍵Cks1kb1、Cks2kb2が通信ネットワーク8を経由して1次ユーザ端末装置4に転送される。このときに必要ならば課金が行われる。なお、暗号化著作権管理プログラムCpks2はデータベース1から供給されるのではなく、ユーザ端末装置4内の例えばROMに内蔵しておくことも可能である。

【0066】データベース1から暗号化原データCm0ks1、2個の暗号化秘密鍵Cks1kb1、Cks2kb2及び暗号化著作権管理プログラムCpks2を受け取った1次ユーザは、データベース組織利用ソフトウェアを利用して第1公開鍵Kb1に対応する第1専用鍵Kv1を用いて暗号化第1秘密鍵Cks1kb1を復号化し、

$$Ks1 = D(Kv1, Cks1kb1)$$

第2公開鍵Kb2に対応する第2専用鍵Kv2を用いて暗号化第2秘密鍵Cks2kb2を復号化する。

$$Ks2 = D(Kv2, Cks2kb2)$$

さらに、復号化された第2秘密鍵Ks2を用いて暗号化著作権管理プログラムCpks2を復号化する。

$$P = D(Ks2, Cpks2)$$

【0067】最後に、復号化された著作権管理プログラムPを利用して復号化された第1秘密鍵Ks1を用いて暗号化データCm0ks1を復号化し、

$$M0 = D(Ks1, Cm0ks1)$$

復号化された原データM0をそのままあるいは加工データM1として利用する。前に説明したように、第1専用鍵Kv1及び第2専用鍵Kv2は1次ユーザが用意他には公開していない暗号鍵であるから、第3者がデータMを入手したとしても暗号化データMを復号化して利用することは不可能である。

【0068】以後原データM0あるいは加工データM1であるデータMの保存、コピーあるいは転送を行う場合には第2秘密鍵Ks2を用いて暗号化及び復号が行われる。

$$Cmks2 = E(Ks2, M)$$

$$M = D(Ks2, Cmks2)$$

復号された第2の秘密鍵Ks2は以後データの保存、コピーあるいは転送を行う場合にデータの暗号化／復号化を行う際の暗号鍵として用いられる。1次ユーザ端末装置4には、これらの第1専用鍵Kv1及び第2専用鍵Kv2、第1の秘密鍵Ks1及び第2秘密鍵Ks2、データM、著作

権管理プログラムPとともに原著作権情報Ic及び1次ユーザがデータの加工を行った場合には1次ユーザ情報及び加工日時等である著作権情報Iclも格納される。なお、この著作権情報Iclは著作権情報ラベルとしてデータに付けるようにし、さらにデジタル署名付にしておけば安全である。暗号化データCmks2は暗号化されて流通し、復号鍵である第2秘密鍵Ks2を入手するためには、著作権情報ラベルが手がかりとなるから、暗号化データCmks2からこの著作権情報ラベルが取り外された場合には、第2秘密鍵Ks2を入手することができない。

【0069】暗号化データCmks2が1次ユーザ端末装置4内に保存された場合には第2の秘密鍵Ks2が装置内に保存されるが、暗号化データCmks2が1次ユーザ端末装置4内に保存されることなく記憶媒体11にコピーあるいは通信ネットワーク8を経由して2次ユーザ端末装置5への転送が行なわれた場合には、1次ユーザ端末装置4における以降の利用を不可能にするために第2の秘密鍵Ks2が廃棄される。なお、この場合コピー・転送回数に制限を設けて、制限回数内のコピー・転送では第2の秘密鍵Ks2が廃棄されないようにしてもよい。

【0070】データMを外部記憶媒体11にコピーあるいは通信ネットワーク8を経由して転送しようとする1次ユーザは、コピーあるいは転送を行うにあたって第2秘密鍵Ks2を用意し、データMを第2の秘密鍵Ks2を用いて暗号化する。

$$Cmks2 = E(Ks2, M)$$

この暗号化データCmks2には暗号化されていない原著作権情報Ic、1次ユーザの著作権情報Iclが付加される。

【0071】2次ユーザは、データベース使用前に1次ユーザと同様に2次ユーザを認証するための認証データAu2、第3の公開鍵Kb3及び第3の公開鍵Kb3に対応する第3の専用鍵Kv3、第4の公開鍵Kb4及び第4の公開鍵Kb4に対応する第4の専用鍵Kv4を用意する。

【0072】コピーあるいは転送された暗号化データCmks2の2次利用を希望する2次ユーザは、2次ユーザ端末装置5を利用して通信ネットワーク8を経由して2次著作権管理センタ14に対して原データ名あるいは原データ番号を指定して2次利用申込を行うが、そのときに、2次ユーザ認証データAu2、原著作権情報Ic及び1次ユーザ著作権情報Iclに加えて第3の公開鍵Kb3と第4の公開鍵Kb4も転送する。

【0073】2次ユーザからの2次利用申込を受けた2次著作権管理センタ14は、2次ユーザの認証データAu2を確認し、確認された2次ユーザ認証データAu2は2次ユーザ情報として3次著作権管理センタ15に転送される。また、1次ユーザの2次著作権情報Iclが転送された場合には2次的著作権情報Iclを2次著作権管理センタ14に照会・確認し、確認された2次的著作権情報Iclは3次著作権管理センタ15に転送される。

【0074】2次著作権管理センタ14は、第3の秘密鍵Ks3を用意する。この第3の秘密鍵Ks3は実施例1に示された鍵センタ9を利用して用意してもよい。用意された第3の秘密鍵Ks3は3次著作権管理センタ15に転送され格納される。

【0075】これらの転送が行われた結果、3次著作権管理センタ15には1次ユーザ著作権情報Icl、1次ユーザ情報I1、原著作権情報Ic、2次ユーザ情報Iu2及び第3の秘密鍵Ks3が格納される。これらの中、1次ユーザ著作権情報Icl及び1次ユーザ情報I1は、著作権使用料金分配に用いられる。

【0076】以下同様にして、n次著作権管理センタ16には(n-1)次ユーザの2次的著作権情報Icn-1、1次ユーザ情報I1、原著作権情報Ic、n次ユーザ情報In及び第nの秘密鍵Ksnが格納される。

【0077】2次著作権管理センタ14から1次ユーザ情報I1、原著作権情報Ic及び第2の秘密鍵Ks2が読み出される。この中、原著作権情報Icは著作権使用料分配のために使用される。読み出された第2の秘密鍵Ks2は2次ユーザの第3の公開鍵Kb3を用いて、第3の秘密鍵Ks3は同じく第4の公開鍵Kb4を用いて暗号化される。

$$Cks2kb3 = E(Kb3, Ks2)$$

$$Cks3kb4 = E(Kb4, Ks3)$$

また、著作権管理プログラムPは第3の秘密鍵Ks3を用いて、第3の秘密鍵Ks3は第4の公開鍵Kb4を用いて暗号化される。

$$Cpks3 = E(Ks3, P)$$

$$Cks3kb4 = E(Kb4, Ks3)$$

暗号化著作権管理プログラムCpks3及び暗号化第2秘密鍵Cks2kb3及び暗号化第3秘密鍵Cks3kb4が通信ネットワーク8を経由して2次ユーザ端末装置3に転送される。このときに必要ならば課金が行われる。

【0078】2次著作権管理センタ14から暗号化された2個の秘密鍵Cks2kb3及びCks3kb4及び暗号化された著作権管理プログラムCpks3を受け取った2次ユーザは、データベース利用ソフトウェアを利用して第3専用鍵Kv3を用いて暗号化第2秘密鍵Cks2kb3を復号し、第4の公開鍵Kb4に対応する第4の専用鍵Kv4を用いて暗号化第3秘密鍵Cks3Kb4を復号する。

$$Ks2 = D(Kv3, Cks2kb3)$$

$$Ks3 = D(Kv4, Cks3kb4)$$

また、復号化された第3の秘密鍵Ks3を用いて暗号化著作権管理プログラムCpks3が復号される。

$$P = D(Ks3, Cpks3)$$

次に、復号化された著作権管理プログラムPを利用して復号された第2の秘密鍵Ks2を用いて暗号化データCmks2を復号化し利用する。

$$M = D(Ks2, Cmks2)$$

【0079】前に説明したように、第3専用鍵Kv3及び

第4専用鍵Kv4は2次ユーザが用意しただけで他には公開していない暗号鍵であるから、第3者が暗号化データCmks2を入手したとしても復号化して利用することは不可能である。

【0080】以上説明した実施例において、データベース1、2次著作権管理センタ14、3次著作権管理センタ15及びn次著作権管理センタ16は、利用申込の輻輳を避けるために別個に設けられている。しかし、利用申込の輻輳が問題とならないならば、これらの全部あるいは一部を合体させることもできる。

【0081】[実施例5] 図3に示されたのは、実施例5のシステム構成であり、この実施例5において、原データは単一のデータベースから暗号化されて一方向的に供給され、ユーザは供給された原データから必要なものを選択して利用する。この実施例において、暗号鍵方式に秘密鍵方式が採用される。

【0082】この図において、1はテキストデータ、コンピュータグラフィックス画面あるいはコンピュータプログラムであるバイナリデータ、デジタル音声データ、デジタル映像データが暗号化された状態で格納されたデータベースであり、2は通信・放送衛星等の人工衛星、3はCD-ROMあるいはフレキシブルディスク等のデータ記録媒体、8は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するCATV回線等の通信ネットワーク、4は1次ユーザ端末装置である。また、17はデータの著作権を管理する著作権管理センタであり、5、6及び7は各々2次ユーザ端末装置、3次ユーザ端末装置及びn次ユーザ端末装置である。

【0083】これらのうちデータベース1、著作権管理センタ17、1次ユーザ端末装置4、2次ユーザ端末装置5、3次ユーザ端末装置6及びn次ユーザ端末装置7は通信ネットワーク8によって相互に接続可能とされている。

【0084】このシステムを利用する各ユーザは予めデータベース組織に登録をしておく必要がある。また、この登録の際にデータベース利用ソフトウェアがユーザに対して提供される。このソフトウェアにはデータ通信プロトコル等の通常の通信ソフトウェアプログラムが含まれている。このデータベース組織を利用するためのソフトウェアは、ユーザ端末装置内の固定ディスクに格納してもよいが、ユーザ端末装置に内蔵されるマスクROM、EPROM、EEPROM等に格納することも可能である。

【0085】また、このシステムにおいてはユーザ側で秘密鍵を生成するため、ユーザ端末装置に秘密鍵生成アルゴリズムが格納されるが、この秘密鍵生成アルゴリズム自身は必ずしも秘密のものではないため、データベース組織に対して利用を登録するときにユーザに対して供給されるデータベース組織利用ソフトウェアに内蔵させ

てもよい。なお、原データが広告付等無料で供給される場合には、暗号化を必要としない場合もあるが、その場合でも著作権は存在するため著作権を使用するための手続きは必要である。

【0086】この図において、破線で示された経路は暗号化されたデータの経路であり、実線で示された経路は各ユーザ端末装置からの要求の経路であり、1点鎖線で示された経路は各データベースから暗号鍵が転送される経路である。

10 【0087】データベース1あるいはデータ記録媒体3に格納されている原データM0は通信ネットワーク8を経由して有線経路で、人工衛星2等經由して放送電波によりあるいは記録媒体3を経由して1次ユーザ端末装置4に供給されるがこのときに第1秘密鍵Ks1を用いて暗号化される。

$$Cm0ks1 = E(Ks1, M0)$$

20 【0088】実施例1～4の場合と同様に、暗号化されて供給される原データCm0ks1の著作権を保護するために、本発明者らによる先願である特願平6-64889号に示されているように、1次ユーザ端末装置4において、原データM0は、表示及び加工のための表示以外の利用形態である保存、コピー、転送が行われるときには第2秘密鍵Ks2を用いて暗号化され、

$$Cm0ks2 = E(Ks2, M0)$$

以後の利用においては第2秘密鍵Ks2によって原データの暗号化/復号化が行われる。

30 【0089】暗号化原データCm0ks1を入手した1次ユーザは1次ユーザ端末装置4を利用して、原データ名あるいは原データ番号等を指定して、暗号化原データCm0ks1の1次利用を著作権管理センタ17に申し込む。1次ユーザ端末装置4から暗号化原データCm0ks1の1次利用申込を受けた著作権管理センタ17は、第1秘密鍵Ks1とともに著作権管理プログラムPを1次ユーザ端末装置4に転送する。この著作権管理プログラムPには暗号アルゴリズムを有する暗号プログラムが含まれており、この暗号プログラムにより秘密鍵の生成及びデータの復号化/暗号化が行われる。

40 【0090】第1秘密鍵Ks1と著作権管理プログラムPを受け取った1次ユーザ端末装置4は、暗号プログラムを利用して第1秘密鍵Ks1を用いて暗号化原データCm0ks1を復号し、

$$M0 = D(Ks1, Cm0ks1)$$

復号化された原データM0をそのままあるいは加工データM1として利用する。また、著作権管理プログラムPにより第1秘密鍵Ks1に基づいて第2秘密鍵Ks2が生成される。

$$Ks2 = P(Ks1)$$

50 【0091】原データM0あるいは加工データM1であるデータMが1次ユーザ端末装置4内に保存される場合、記録媒体11に複写される場合、2次ユーザ端末装置5



に転送される場合には、著作権管理プログラムPにより第2秘密鍵Ks2を用いて暗号化される。

$$Cmks2 = E(Ks2, M)$$

【0092】第2秘密鍵Ks2によって暗号化されたデータCmks2は、原データ名あるいは原データ番号とともに、記録媒体11に複写あるいは通信ネットワーク8を経由して2次ユーザ端末装置5に転送される。

【0093】暗号化されたデータCmks2を入手した2次ユーザは2次ユーザ端末装置5を利用して、原データ名あるいは原データ番号を指定することにより暗号化データCmks2の2次利用を著作権管理センタ17に申し込む。

【0094】暗号化データCmks2の2次利用申込を受けた著作権管理センタ17は、原データ名あるいは原データ番号から第1秘密鍵Ks1を探し出し、著作権管理プログラムPにより第1秘密鍵Ks1から第2秘密鍵Ks2を生成し、

$$Ks2 = P(Ks1)$$

生成された第2秘密鍵Ks2を著作権管理プログラムPとともに2次ユーザ端末装置5に供給する。

【0095】第2秘密鍵Ks2と著作権管理プログラムPを受け取った2次ユーザ端末装置5は、第2秘密鍵Ks2で暗号化されたデータCmks2を第2秘密鍵Ks2で復号化して

$$M = D(Ks2, Cmks2)$$

表示あるいは加工の利用を行う。

【0096】復号されたデータMが2次ユーザ端末装置5内に保存される場合、記録媒体12に保存される場合、通信ネットワーク8を経由して3次ユーザ端末装置6に転送される場合には、そのデータMは著作権管理プログラムPにより第2秘密鍵Ks2を用いて暗号化される。

【0097】さらに、著作権管理プログラムPが、第2秘密鍵Ks2に基づいて第3秘密鍵Ks3を生成するようにし、

$$Ks3 = P(Ks2)$$

【0098】データMが2次ユーザ端末装置5内に保存される場合、記録媒体12に複写される場合、通信ネットワーク8を経由して3次ユーザ端末装置6に転送される場合には、そのデータMは著作権管理プログラムPにより第3の秘密鍵Ks3を用いて暗号化されるようにしてもよい。

$$Cmks3 = E(Ks3, M)$$

【0099】〔実施例6〕次に、実施例6について説明するが、実施例5と同様に原データは単一のデータベースから暗号化されて一方向的に供給され、ユーザは供給された原データから必要なものを選択して利用する。この実施例において採用される暗号鍵方式は秘密鍵方式であり、第2秘密鍵は1次ユーザ情報と第1秘密鍵に基づいて生成される。なお、実施例6で用いるシステム構成

は図3に示された実施例5のシステム構成と異なる点はないため、システム構成についての説明は省略する。

【0100】実施例6において、データベース1に格納されている原データM0は通信ネットワーク8を経由して有線経路で、人工衛星2等經由して放送電波によりあるいは記録媒体3を経由して第1秘密鍵Ks1を用いて暗号化されて

$$Cm0ks1 = E(Ks1, M0)$$

1次ユーザ端末装置4に供給される。

【0101】暗号化原データCm0ks1を入手した1次ユーザは1次ユーザ端末装置4を利用して、暗号化原データCm0ks1の1次利用を著作権管理センタ17に申し込むが、このときに原データ名あるいは原データ番号等を指定するとともに1次ユーザ情報Iu1を提示する。

【0102】1次ユーザから暗号化原データCm0ks1の1次利用申込を受けた著作権管理センタ17は、第1秘密鍵Ks1と著作権管理プログラムPを1次ユーザ端末装置4に供給する。

【0103】著作権管理プログラムPには、暗号アルゴリズムを有する暗号プログラムPが含まれており、この暗号プログラムPにより秘密鍵生成及び復号/暗号化が行われる。

【0104】第1秘密鍵Ks1と著作権管理プログラムを受け取った1次ユーザ端末装置4では、暗号プログラムPにより第1秘密鍵Ks1を用いて暗号化原データM0を復号して

$$M0 = D(Ks1, Cm0ks1)$$

復号化された原データM0をそのままあるいは加工データM1として利用する。また、供給された著作権管理プログラムPが、1次ユーザ情報Iu1あるいは1次ユーザ情報Iu1と第1秘密鍵Ks1に基づいて第2秘密鍵Ks2を生成する。

$$Ks2 = P(Iu1) \quad \text{又は}$$

$$Ks2 = P(Iu1 + Ks1)$$

生成された第2秘密鍵Ks2は1次ユーザ情報Iu1に基づいているため、正しい1次ユーザ情報Iu1を有していなければ生成することが不可能である。なお、1次ユーザ情報Iu1に代えて、1次ユーザ情報Iu1に基づいて生成された1次ユーザデータ、あるいは1次ユーザ端末装置4に付与されている装置番号を利用することもできる。

【0105】原データM0あるいは加工データM1であるデータMが1次ユーザ端末装置4内に保存される場合、記録媒体11に複写される場合、通信ネットワーク8を経由して2次ユーザ端末装置5に供給される場合には、そのデータMは著作権管理プログラムPにより第2秘密鍵Ks2を用いて暗号化される。

$$Cmks2 = E(Ks2, M)$$

【0106】第2秘密鍵Ks2で暗号化されたデータCmks2は、原データ名あるいは原データ番号及び1次ユーザ情報Iu1とともに、記録媒体11に複写されあるいは、

通信ネットワーク 8 を経由して 2 次ユーザ端末装置 5 に供給される。

【0107】暗号化されたデータ  $C_{mks2}$  を入手した 2 次ユーザは 2 次ユーザ端末装置 5 を利用して、データ  $M$  の 2 次利用を著作権管理センタ 17 に申し込むが、このときに原データ名あるいは原データ番号等を指定するとともに 1 次ユーザ情報  $I_{u1}$  を提示する。

【0108】データ  $M$  の 2 次利用申込を受けた著作権管理センタ 17 は、原データ名あるいは原データ番号を手がかりとして第 1 秘密鍵  $K_{s1}$  を探し出し、1 次ユーザ情報  $I_{u1}$ 、第 1 秘密鍵  $K_{s1}$  あるいは 1 次ユーザ情報  $I_{u1}$  と第 1 秘密鍵  $K_{s1}$  に基づいて第 2 秘密鍵  $K_{s2}$  を生成し、生成された第 2 秘密鍵  $K_{s2}$  を著作権管理プログラム  $P$  とともに 2 次ユーザ端末装置 5 に提供する。

【0109】第 2 秘密鍵  $K_{s2}$  と著作権管理プログラム  $P$  を受け取った 2 次ユーザは 2 次ユーザ端末装置 5 を利用して、著作権管理プログラム  $P$  により第 2 秘密鍵  $K_{s2}$  を用いて暗号化データ  $C_{mks2}$  を復号化して利用する。  
 $M = D(K_{s2}, C_{mks2})$

データ  $M$  が 2 次ユーザ端末装置 5 内に保存される場合、記録媒体 11 に複写される場合、通信ネットワークを経由して 3 次ユーザ端末装置 6 に供給される場合には、そのデータは第 2 秘密鍵  $K_{s2}$  によって暗号化される。

【0110】なお、著作権管理プログラム  $P$  により第 2 秘密鍵  $K_{s2}$  に基づいて第 3 秘密鍵  $K_{s3}$  を生成するようにし、

$$K_{s3} = P(K_{s2})$$

データ  $M$  が 2 次ユーザ端末装置 5 内に保存される場合、記録媒体 11 に複写される場合、通信ネットワークを経由して 3 次ユーザ端末装置 6 に供給される場合には、そのデータは第 3 秘密鍵  $K_{s3}$  によって暗号化されるようにすることもできる。

【0111】また、2 次ユーザが著作権管理センタ 17 に 2 次利用申込を行うときに、2 次ユーザ情報  $I_{u2}$  を提示し、提示された 2 次ユーザ情報  $I_{u2}$  に基づいて第 3 秘密鍵  $K_{s3}$  が生成されるようにすることもできる。

【0112】この実施例 6 において、第 2 秘密鍵  $K_{s2}$  を生成する著作権管理プログラム  $P$  を全データベース組織において共通のものとしておけば、どのデータベース組織においても 1 次ユーザ情報  $I_{u1}$  及び第 1 秘密鍵  $K_{s1}$  が変更されない限り同一の原データに対しては同一の第 2 秘密鍵  $K_{s2}$  が生成される。

【0113】〔実施例 7〕次に、実施例 7 について説明するが、実施例 5 及び実施例 6 と同様に原データは単一のデータベースから暗号化されて 1 方向的に供給され、ユーザは供給された原データから必要なものを選択して利用する。また、この実施例において第 2 秘密鍵は著作権管理プログラムの使用回数と第 1 秘密鍵に基づいて生成される。

【0114】この実施例において採用される暗号鍵方式

は秘密鍵方式である。なお、実施例 7 で用いるシステム構成は図 3 に示された実施例 5 及び実施例 6 のシステム構成と異なる点はないため、システム構成についての説明は省略する。

【0115】データベース 1 に格納されている原データ  $M0$  は通信ネットワーク 8 を経由して有線経路で、人工衛星 2 等を経由して放送電波によりあるいは記録媒体 3 を経由して第 1 秘密鍵  $K_{s1}$  を用いて暗号化されて  
 $C_{m0ks1} = E(K_{s1}, M0)$

1 次ユーザ端末装置 4 に供給される。

【0116】暗号化原データ  $C_{m0ks1}$  を入手した 1 次ユーザは 1 次ユーザ端末装置 4 を利用して、原データ名あるいは原データ番号等を指定することにより原データ  $M0$  の 1 次利用を著作権管理センタ 17 に申し込む。

【0117】原データ  $M0$  の 1 次利用申込を受けた著作権管理センタ 17 は、第 1 秘密鍵  $K_{s1}$  及び著作権管理プログラム  $P$  を 1 次ユーザ端末装置 4 に転送する。

【0118】この著作権管理プログラム  $P$  には暗号アルゴリズムを有する暗号プログラムが含まれており、暗号鍵の生成及びデータの復号化／暗号化が行われる。また、著作権管理プログラム  $P$  にはカウンタが付属しており、このカウンタがプログラム  $P$  の使用回数  $N$  を計数する。

【0119】第 1 秘密鍵  $K_{s1}$  及び著作権管理プログラム  $P$  を受け取った 1 次ユーザは、暗号化原データ  $C_{m0ks1}$  を著作権管理プログラム  $P$  を利用して第 1 秘密鍵  $K_{s1}$  を用いて復号化して

$$M0 = D(K_{s1}, C_{m0ks1})$$

復号化された原データ  $M0$  をそのままあるいは加工データ  $M1$  として利用する。

【0120】このシステムにおいては、データの著作権を管理するために原データ  $M0$  あるいは加工データ  $M1$  であるデータ  $M$  が 1 次ユーザ端末装置 4 内に保存される場合、記録媒体 11 に複写される場合、通信ネットワーク 8 を経由して 2 次ユーザ端末装置 5 に転送される場合に著作権管理プログラムに  $P$  より第 2 秘密鍵  $K_{s1}$  を用いて暗号化されるが、このときに用いられる第 2 暗号鍵  $K_{s2}$  は著作権管理プログラムの使用回数  $N$  と第 1 秘密鍵  $K_{s1}$  に基づいて生成される。

$$K_{s2} = P(N + K_{s1})$$

【0121】このようにして生成される第 2 秘密鍵  $K_{s2}$  は著作権管理プログラム  $P$  の使用回数  $N$  と第 1 秘密鍵  $K_{s1}$  に基づいているため、データ  $M$  は利用される度に最新の第 2 秘密鍵  $K_{s2}$  で暗号化される。

$$C_{mks2} = E(K_{s2}, M)$$

【0122】最後の利用によって生成された第 2 秘密鍵  $K_{s2}$  によって暗号化されたデータ  $C_{mks2}$  は、原データ名あるいは原データ番号、カウンタデータ  $N1$  とともに、記録媒体 11 に複写あるいは、通信ネットワーク 8 を経由して 2 次ユーザ端末装置 5 に転送される。

【0123】暗号化データCmks2を入手した2次ユーザは2次ユーザ端末装置5を用いて、原データ名あるいは原データ番号及びカウンタデータN1を提示して、暗号化データCmks2の2次利用を著作権管理センタ17に申し込む。

【0124】暗号化データCmks2の2次利用申込を受けた著作権管理センタ17は、提示された原データ名あるいは原データ番号から第1秘密鍵Ks1を探し出し、カウンタデータN1及び第1秘密鍵Ks1に基づいて第2秘密鍵Ks2を生成し、著作権管理プログラムPとともに第2秘密鍵Ks2を通信ネットワーク8を経由して2次ユーザ端末装置5に供給する。

【0125】第2秘密鍵Ks2と著作権管理プログラムPを受け取った2次ユーザは、暗号化データCmks2を著作権管理プログラムPを利用して第2秘密鍵Ks2を用いて復号化し

$$M = D(Ks2, Cmks2)$$

復号化されたデータMをそのままあるいは加工して利用する。

【0126】データMが2次ユーザ端末装置5内に保存される場合、記録媒体11に複写される場合、通信ネットワーク8を経由して3次ユーザ端末装置6に転送される場合には、データMは著作権管理プログラムPにより第2秘密鍵Ks2によって暗号化される。

$$Cmks2 = E(Ks2, M)$$

【0127】この場合、さらに著作権管理プログラムPが、2次ユーザ端末装置5における著作権管理プログラムPの使用回数N2と秘密鍵Ks2に基づいて第3秘密鍵Ks3を生成するようにすることもできる。

$$Ks3 = P(N2 + Ks2)$$

この場合、データMが2次ユーザ端末装置5内に保存される場合、記録媒体11に複写される場合、通信ネットワーク8を経由して3次ユーザ6に転送される場合には、データMは著作権管理プログラムPにより第3秘密鍵Ks3によって暗号化される。

$$Cmks3 = E(Ks3, M)$$

【0128】〔実施例8〕図4に示されたのは、データ著作権管理システムの実施例8のシステム構成であり、この実施例8において単一のデータベースから供給される原データはユーザからの要求に応じて双方向的に供給される。この実施例において採用される暗号方式は秘密鍵方式であり、第1秘密鍵に基づいて第2秘密鍵が生成される。

【0129】この図において、1はデータベース、4は1次ユーザ端末装置、5は2次ユーザ端末装置、6は3次ユーザ端末装置、7はn次ユーザ端末装置である。また、18は著作権管理センタ、8は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するCATV回線等の通信ネットワークである。

【0130】これらのうちデータベース1、著作権管理

センタ18、1次ユーザ端末装置4、2次ユーザ端末装置5、3次ユーザ端末装置6及びn次ユーザ端末装置7は通信ネットワーク8によって相互に接続可能とされている。

【0131】このシステムを利用する各ユーザは予めデータベース組織に登録をしておく必要がある。また、この登録の際にデータベース組織用ソフトウェアがユーザに対して提供される。このソフトウェアにはデータ通信用プロトコル等の通常の通信用ソフトウェアプログラムが含まれている。このデータベース組織用ソフトウェアは、ユーザ端末装置内の固定ディスクに格納してもよいが、ユーザ端末装置に内蔵されるマスクROM、EPROM、EEPROM等に格納することも可能である。

【0132】また、このシステムにおいてはユーザ側で秘密鍵を生成するためユーザ端末装置に秘密鍵生成アルゴリズムが格納されるが、この秘密鍵生成アルゴリズム自身は必ずしも秘密のものではないため、データベース組織に登録するときユーザに対して提供されるデータベース組織用ソフトウェアに内蔵させてもよい。なお、広告付等の無料で供給される原データの場合には、暗号化を必要としない場合もあるが、その場合でも著作権は存在するため著作権を使用するための手続きは必要である。

【0133】なお、この図において、破線で示された経路は暗号化されたデータの経路であり、実線で示された経路は各ユーザ端末装置からの要求の経路であり、1点鎖線で示された経路は各データベースからの利用形態に対応した利用許可情報及び著作権管理プログラムとともに秘密鍵が転送される経路である。

【0134】この図において、データベース1にはテキストデータ、グラフィックスデータあるいはバイナリデータ、音声データ、映像データが暗号化されていない状態で保管されている。

【0135】1次ユーザは1次ユーザ端末装置4を使用して通信ネットワーク8を経由してデータベース1に対して、利用することを希望する原データ名を指定して原データM0の利用を申し込む。

【0136】1次ユーザ端末装置4から原データM0の利用申し込みを受けたデータベース1は、原データM0を第1秘密鍵Ks1で暗号化し、

$$Cm0ks1 = E(Ks1, M0)$$

暗号化された原データCm0ks1及び第1秘密鍵Ks1とともに著作権管理プログラムPを1次ユーザ端末装置4に供給する。この著作権管理プログラムPには暗号アルゴリズムを有する暗号プログラムが含まれており、この暗号プログラムPにより、秘密鍵の生成及びデータの復号化/暗号化が行われる。なお、この暗号アルゴリズムを第1秘密鍵Ks1に依存するものにしておけば、著作権管理プログラムPをその原データM0に固有のものとすることができる。



【0137】第1秘密鍵 $K_{s1}$ を用いて暗号化された原データ $C_{m0ks1}$ とともに第1秘密鍵 $K_{s1}$ と著作権管理プログラム $P$ を受け取った1次ユーザ端末装置4は、第1秘密鍵 $K_{s1}$ を用いて暗号化原データ $C_{m0ks1}$ を復号し、 $M0 = D(K_{s1}, C_{m0ks1})$

復号化された原データ $M0$ をそのままあるいは加工データ $M1$ として利用する。また、著作権管理プログラム $P$ により、第1秘密鍵 $K_{s1}$ に基づいて第2秘密鍵 $K_{s2}$ が生成される。

$K_{s2} = P(K_{s1})$

【0138】復号された原データあるいは加工されたデータであるデータ $M$ が1次ユーザ端末装置4内に保存される場合、記録媒体11に複写される場合、通信ネットワーク8を経由して2次ユーザ端末装置5に転送される場合には、そのデータ $M$ は著作権管理プログラム $P$ により第2秘密鍵 $K_{s2}$ を用いて暗号化される。

$C_{mks2} = E(K_{s2}, M)$

【0139】暗号化データ $C_{mks2}$ は、原データ名あるいは原データ番号とともに、記録媒体11に複写され、あるいは、通信ネットワーク8を経由して2次ユーザ端末装置5に転送される。

【0140】暗号化データ $C_{mks2}$ を入手した2次ユーザは、2次ユーザ端末装置5を利用して、原データ名あるいは原データ番号を指定することにより原データあるいは加工データであるデータ $M$ の2次利用を著作権管理センタ18に申し込む。

【0141】データ $M$ の2次利用申込を受けた2次著作権管理センタ18は、原データ名あるいは原データ番号を手がかりとして第1秘密鍵 $K_{s1}$ を探し出し、第1秘密鍵 $K_{s1}$ に基づいて第2秘密鍵 $K_{s2}$ を生成し、 $K_{s2} = P(K_{s1})$

生成された第2秘密鍵 $K_{s2}$ を著作権管理プログラム $P$ とともに2次ユーザ端末装置5に供給する。

【0142】第2秘密鍵 $K_{s2}$ と著作権管理プログラム $P$ を受け取った2次ユーザ端末装置5は、暗号化データ $C_{mks2}$ を著作権管理プログラム $P$ を利用して第2秘密鍵 $K_{s2}$ を用いて復号化して $M = D(K_{s2}, C_{mks2})$

復号化された $M$ をそのままあるいは加工して利用する。データ $M$ が2次ユーザ端末装置5内に保存される場合、記録媒体12に複写される場合、通信ネットワーク8を経由して3次ユーザ端末装置6に転送される場合には、

【0143】著作権管理プログラム $P$ により第2秘密鍵 $K_{s2}$ に基づいて第3秘密鍵 $K_{s3}$ が生成され、 $K_{s3} = P(K_{s2})$

著作権管理プログラム $P$ によりこの生成された第3秘密鍵 $K_{s3}$ を用いてデータ $M$ が暗号化される。

$C_{mks3} = E(K_{s3}, M)$

【0144】〔実施例9〕次に説明する実施例9は図4に示された実施例8と同様に単一のデータベースから供

給される原データはユーザからの要求に応じて供給される。この実施例において採用される暗号方式は秘密鍵方式であり、第2秘密鍵の生成に実施例8で用いられた第1秘密鍵に加えてユーザデータを利用する。なお、この実施例のシステム構成は実施例8のシステム構成と異なる点はないので、システム構成についての説明は省略する。

【0145】データベース1には、原データ $M0$ が暗号化されていない状態で保管されている。1次ユーザが1次ユーザ端末装置4を利用してデータベース1にアクセスすると、データメニューが転送される。このときデータメニューとともに料金の情報を表示してもよい。

【0146】データメニューが転送されると1次ユーザはデータメニュー検索を行い原データ $M0$ を選択し、選択した原データ $M0$ の原データ名等を指定することによりデータベース1に対して、原データ $M0$ の1次利用を申し込む。

【0147】1次ユーザ端末装置4から原データ $M0$ の利用申し込みを受けたデータベース1では、原データ $M0$ が読み出され、読み出された原データ $M0$ が第1秘密鍵 $K_{s1}$ で暗号化され、 $C_{m0ks1} = E(K_{s1}, M0)$

暗号化された原データ $C_{m0ks1}$ 及び第1秘密鍵 $K_{s1}$ とともに著作権管理プログラム $P$ を1次ユーザ端末装置4に供給される。

【0148】ここで使用される著作権管理プログラム $P$ は全てのデータベース組織において共通のものであり、さらに暗号アルゴリズムを有する暗号プログラムを含んでおり、この暗号プログラムにより暗号生成及びデータの復号化／暗号化が行われる。

【0149】第1秘密鍵 $K_{s1}$ と著作権管理プログラム $P$ を受け取った1次ユーザ端末装置4は、著作権管理プログラム $P$ により第1秘密鍵 $K_{s1}$ を用いて暗号化された原データ $C_{m0ks1}$ を復号化して $M0 = D(K_{s1}, C_{m0ks1})$

復号化された原データ $M0$ をそのままあるいは加工データ $M1$ として利用する。また、著作権管理プログラム $P$ が、1次ユーザ情報 $I_{u1}$ に基づいて第2の秘密鍵 $K_{s2}$ を生成する。

$K_{s2} = P(I_{u1})$

この第2の秘密鍵 $K_{s2}$ は、1次ユーザ情報 $I_{u1}$ 以外に第1秘密鍵 $K_{s1}$ あるいは1次ユーザデータ $I_{u1}$ と第1秘密鍵 $K_{s1}$ とに基づいて生成することもできる。

$K_{s2} = P(K_{s1})$

$K_{s2} = P(K_{s1} + I_{u1})$

【0150】原データ $M0$ あるいは加工データ $M1$ であるデータ $M$ が1次ユーザ端末装置4内に保存される場合、記録媒体11に複写される場合、通信ネットワーク8を経由して2次ユーザ端末装置5に転送される場合には、そのデータ $M$ は著作権管理プログラム $P$ により第2の秘

密鍵Ks2によって暗号化される。

$$Cmks2 = E(Ks2, M)$$

【0151】第2の秘密鍵Ks2によって暗号化されたデータCmks2は、原データ名あるいは原データ番号が付されるとともに、記録媒体11に複写されあるいは、通信ネットワーク8を経由して2次ユーザ端末装置5に転送される。

【0152】第2秘密鍵Ks2によって暗号化されたデータCmks2を入手した2次ユーザは、2次ユーザ端末装置5を利用してデータMの2次利用を著作権管理センタ18に申し込むが、このときに原データ名あるいは原データ番号等を指定するとともに暗号化されていない1次ユーザ情報Iu1を提示する。

【0153】データMの2次利用申込を受けた著作権管理センタ18は、指定された原データ名あるいは原データ番号により第1秘密鍵Ks1を探し出し、著作権管理プログラムPにより提示された1次ユーザ情報Iu1、探し出された第1秘密鍵Ks1に基づいて第2秘密鍵Ks2を生成し、著作権管理プログラムPとともに2次ユーザ端末装置5に供給する。

【0154】第2秘密鍵Ks2と著作権管理プログラムPを受け取った2次ユーザは2次ユーザ端末装置5を利用して、著作権管理プログラムPにより第2の秘密鍵Ks2を用いて暗号化されたデータCmks2を復号化して、  

$$M = D(Ks2, Cmks2)$$

復号化されたデータMをそのままあるいは加工して利用する。データMが2次ユーザ端末装置5内に保存される場合、記録媒体11に複写される場合、通信ネットワーク8を経由して3次ユーザ端末装置6に転送される場合には、そのデータMは著作権管理プログラムPにより第2の秘密鍵Ks2によって暗号化される。

$$Cmks2 = E(Ks2, M)$$

【0155】なお、この場合、著作権管理プログラムPが、1次ユーザ情報Iu1、第2秘密鍵Ks2あるいは1次ユーザ情報Iu1と第2秘密鍵Ks2に基づいて第3の秘密鍵Ks3を生成する

$$Ks3 = P(Iu1)$$

$$Ks3 = P(Iu1 + Ks1)$$

$$Ks3 = P(Ks1)$$

ようにすることもできる。また、2次ユーザが2次利用申込を行うときに2次ユーザ情報Iu2を提示し、1次ユーザ情報Iu1の代わりに2次ユーザ情報Iu2に基づいて第3秘密鍵を生成することもできる。データMは著作権管理プログラムPにより第3秘密鍵Ks3によって暗号化される。

$$Cmks3 = E(Ks3, M)$$

【0156】この実施例において、第2秘密鍵Ks2を生成する著作権管理プログラムPは全データベース組織において共通のものであるから、どのデータベース組織においても、1次ユーザデータIu1及び第1秘密鍵Ks1が

変更されない限り同一の原データに対しては同一の第2秘密鍵Ks2が生成される。

【0157】〔実施例10〕次に説明する実施例10は図4に示された実施例8と同様に原データが単一のデータベースからユーザからの要求に応じて供給される。この実施例において採用される暗号方式は秘密鍵方式である。この実施例においては、第2秘密鍵の生成に実施例9で用いられたユーザ情報に代えて著作権管理プログラムの使用回数を利用する。なお、この実施例のシステム構成は実施例8のシステム構成と異なる点はないので、システム構成についての説明は省略する。

【0158】データベース1には、原データM0が暗号化されていない状態で保管されている。1次ユーザが1次ユーザ端末装置4を利用してデータベース1にアクセスすると、データメニューが転送される。このときデータメニューとともに料金の情報を表示してもよい。

【0159】データメニューが転送されると1次ユーザはデータメニュー検索を行い原データM0を選択し、1次ユーザ端末装置4を利用して、通信ネットワーク8を経由してデータベース1に対して、原データ名等を指定して1次利用を希望する原データM0の利用を申し込む。

【0160】1次ユーザからデータ利用申し込みを受けたデータベース1は、原データM0を第1秘密鍵Ks1で暗号化し、

$$Cm0ks1 = E(Ks1, M0)$$

暗号化されたデータCm0ks1と第1秘密鍵Ks1とともに著作権管理プログラムPを1次ユーザ端末装置4に供給する。

【0161】この著作権管理プログラムPには暗号アルゴリズムを有する暗号プログラムが含まれており、この暗号プログラムにより暗号鍵生成及びデータの復号化/暗号化が行われる。また、著作権管理プログラムPにはカウンタが付属しており、このカウンタがプログラムの使用回数Nあるいは原データの利用回数Nを計数する。なお、この暗号アルゴリズムを第1秘密鍵Ks1に依存するものにしておけば、著作権管理プログラムPをその原データ固有のものとすることができる。

【0162】第1秘密鍵Ks1と著作権管理プログラムPを受け取った1次ユーザは、暗号化された原データCm0ks1を著作権管理プログラムPを使用して第1秘密鍵Ks1を用いて復号化して、

$$M0 = D(Ks1, Cm0ks1)$$

復号化された原データM0をそのままあるいは加工データM1として利用する。

【0163】データの著作権を保護するため、原データM0あるいは加工データM1であるデータMが1次ユーザ端末装置4内に保存される場合、記録媒体11に複写される場合、通信ネットワーク8を経由して2次ユーザ端末装置5に転送される場合には、そのデータMは著作権

管理プログラムPにより暗号化される。言い換えれば、これらの利用が行われるときには必ず著作権管理プログラムが動作する。

【0164】一方、供給された著作権管理プログラムPが使用されるとプログラム内のカウンタが計数を行い、そのカウント数Nと第1秘密鍵Ks1に基づいて著作権管理プログラムPが第2秘密鍵Ks2を生成する。

$$Ks2 = P(N + Ks1)$$

【0165】この第2秘密鍵Ks2は著作権管理プログラムPの使用回数Nにも基づいているため、データMは利用される度に新しい第2秘密鍵Ks2で暗号化される。

$$Cmks2 = E(Ks2, M)$$

最後に生成された第2秘密鍵Ks2によって暗号化されたデータCmks2は、原データ名あるいは原データ番号、1次ユーザ情報Iu1及びカウンタデータNとともに、記録媒体11に複写あるいは、通信ネットワーク8を経由して2次ユーザ端末装置5に転送される。

【0166】第2秘密鍵Ks2を用いて暗号化されたデータCmks2を入手した2次ユーザは、原データ名あるいは原データ番号、1次ユーザ情報Iu1及びカウンタデータNを提示して、データMの2次利用を著作権管理センタ18に申し込む。

【0167】暗号化されたデータCmks2の2次利用申込を受けた著作権管理センタ18は、そのデータの原データ名あるいは原データ番号から第1の秘密鍵Ks1を探し出し、第1の秘密鍵、提示された1次ユーザ情報Iu1及びカウンタデータNから第2の秘密鍵Ks2を生成し、生成された第2の秘密鍵Ks2を著作権管理プログラムPとともに2次ユーザ端末装置5に転送する。

【0168】第2の秘密鍵Ks2と著作権管理プログラムPを受け取った2次ユーザ端末装置5は、著作権管理プログラムPを利用して暗号化データCmks2を第2の秘密鍵Ks2を用いて復号化し

$$M = D(Ks2, Cmks2)$$

復号化されたデータMをそのままあるいは加工して利用する。

【0169】データが2次ユーザ端末装置5内に保存される場合、記録媒体12に複写される場合、通信ネットワーク8を経由して3次ユーザ端末装置6に転送される場合には、そのデータは著作権管理プログラムにより第2の秘密鍵によって暗号化される。

【0170】なお、さらに著作権管理プログラムが、第2の秘密鍵に基づいて第3の秘密鍵を生成することもできる。

【0171】以上説明した実施例1から実施例10はいずれもデータベースから供給された単一原データを利用する場合についてのものである。しかし、データの利用形態としての加工には単一のデータを加工する他に、同一のデータベースから入手した複数の原データを組み合わせて新しいデータを作成する場合及び複数のデータベ

ースから入手した複数の原データを組み合わせて新しいデータを作成する場合がある。

【0172】[実施例11]次に説明する実施例11は、1次ユーザが単一のデータベースに保存されている複数の原データを組み合わせて新しいデータを作成する実施例であり、1次ユーザはデータベースに保存されている第1、第2、第3の原データを材料にして新しいデータを作成する。

【0173】この実施例においては図4に示された実施例8と同様に複数の原データが単一のデータベースからユーザの要求に応じて供給される。この実施例において採用される暗号方式は秘密鍵方式である。なお、この実施例のシステム構成は実施例8のシステム構成と異なる点はないので、システム構成についての説明は省略する。

【0174】データベース1には、原データM01, M02, M03が暗号化されていない状態で保管されている。1次ユーザが1次ユーザ端末装置4を利用してデータベース1にアクセスすると、データメニューが転送される。このときデータメニューとともに料金の情報を表示してもよい。

【0175】データメニューが転送されると1次ユーザはデータメニュー検索を行い原データM01, M02, M03を選択し、1次ユーザ端末装置4を利用して、通信ネットワーク8を経由してデータベース1に対して、第1、第2、第3の原データM01, M02, M03の原データ名あるいは原データ番号を指定して各原データの供給を申し込むがこのときに1次ユーザ情報Iu1を提示する。

【0176】1次ユーザから第1、第2、第3の原データM01, M02, M03の供給申し込みを受けたデータベース1は、供給申込を受けた第1、第2、第3の原データM01, M02, M03を各々第1、第2、第3の秘密鍵Ks01, Ks02, Ks03を用いて暗号化し、

$$Cm01ks01 = E(Ks01, M01)$$

$$Cm02ks02 = E(Ks02, M02)$$

$$Cm03ks03 = E(Ks03, M03)$$

第1、第2、第3の秘密鍵Ks01, Ks02, Ks03及び全てのデータベース組織と全ての原データに共通する著作権管理プログラムPを1次ユーザ端末装置4に供給する。この著作権管理プログラムPには暗号アルゴリズムを有する暗号プログラムが含まれており、暗号鍵生成及び復号化/暗号化が行われる。

【0177】暗号化第1原データCm01ks01, 暗号化第2原データCm02ks02, 暗号化第3原データCm03ks03, 第1秘密鍵Ks01, 第2秘密鍵Ks02, 第3秘密鍵Ks03, 著作権管理プログラムPを受け取った1次ユーザ端末装置4は、著作権管理プログラムPを利用してこれらの秘密鍵Ks01, Ks02, Ks03を用いて第1、第2、第3の各暗号化原データCm01ks01, Cm02ks02, Cm03ks03を復号化し



$M01 = D(Ks01, Cm01ks01)$

$M02 = D(Ks02, Cm02ks02)$

$M03 = D(Ks03, Cm03ks03)$

原データM01, M02, M03を加工して新しいデータM1を作成する。

【0178】また、著作権管理プログラムPが第1秘密鍵Ks01, 第2秘密鍵Ks02, 第3秘密鍵Ks03, 1次ユーザデータIulのうちの1つあるいはこの中のいくつかに基づいて第4秘密鍵Ks4を生成する。

$Ks4 = P(Ks01/Ks02/Ks03/Iul)$

【0179】加工データM1が1次ユーザ端末装置4内に保存される場合、記録媒体11に複写される場合、通信ネットワーク8を経由して2次ユーザ5に転送される場合には、著作権管理プログラムPにより第4秘密鍵Ks4によって暗号化される。

$Cm1ks4 = E(Ks4, M1)$

【0180】暗号化加工データCm1ks4は原データ名あるいは原データ番号及び1次ユーザデータIulとともに、記録媒体11に複写あるいは通信ネットワーク8を経由して2次ユーザ端末装置5に転送される。

【0181】暗号化加工データCm1ks4を入手した2次ユーザは2次ユーザ端末装置5を利用して暗号化加工データCm1ks4の2次利用を著作権管理センタ18に申し込むが、このときに原データM01, M02, M03のデータ名あるいはデータ番号等を指定するとともに1次ユーザ情報Iulを提示する。

【0182】2次ユーザから暗号化加工データCm1ks4の2次利用申込を受けた著作権管理センタ18は、第1原データM01のデータ名あるいはデータ番号から第1秘密鍵Ks01を探し出し、第2原データM02のデータ名あるいはデータ番号から第2秘密鍵Ks02を探し出し、第3原データM03のデータ名あるいは原データ番号から第3秘密鍵Ks03を探し出し、共通の著作権管理プログラムPにより、探し出された第1秘密鍵Ks01, 第2秘密鍵Ks02, 第3秘密鍵Ks03, 1次ユーザ情報Iulのうちの1つあるいはこの中のいくつかに基づいて第4秘密鍵Ks4を生成し、

$Ks4 = P(Ks01/Ks02/Ks03/Iul)$

共通の著作権管理プログラムPとともに2次ユーザ5に提供する。

【0183】第4の秘密鍵と共通の著作権管理プログラムを受け取った2次ユーザは、著作権管理プログラムPにより第4秘密鍵Ks4を用いて加工データM1を復号化し

$M1 = D(Ks4, Cm1ks4)$

復号化された加工データM1をそのままあるいは再加工データM2として利用する。

【0184】加工データM1あるいは再加工データM2が2次ユーザ端末装置5内に保存される場合、記録媒体12に複写される場合あるいは通信ネットワーク8を経由

して3次ユーザ6に転送される場合には、著作権管理プログラムPにより第4秘密鍵Ks4に基づいて第5秘密鍵Ks5が生成され、

$Ks5 = P(Ks4)$

それらのデータは著作権管理プログラムPにより第5秘密鍵Ks5を用いて暗号化される。

$Cm1ks5 = E(Ks5, Cm1)$

$Cm2ks5 = E(Ks5, Cm2)$

【0185】なお、共通の著作権管理プログラムPが、第4秘密鍵Ks4を用いて第5秘密鍵Ks5を生成し、生成された第5秘密鍵Ks5を用いて以後の暗号化/復号化を行うようにすることもできる。

【0186】この実施例において、第4の秘密鍵を生成する著作権管理プログラムは全データベース組織において共通のものであるから、どのデータベース組織においても、1次ユーザデータ及び第1の秘密鍵が変更されない限り同一の原データに対しては同一の第4の秘密鍵が生成される。

【0187】この実施例における、共通の著作権管理プログラムは著作権管理センタ18から供給されるが、各ユーザ端末装置内のROMに内蔵、あるいはデータベースを利用するためのソフトウェアに内蔵してもよい。

【0188】〔実施例12〕次に説明する実施例12では、複数のデータベースからユーザの要求に応じて供給される複数の原データを組み合わせて新しいデータを作成する実施例であり、この実施例においては暗号鍵方式として秘密鍵方式が採用される。

【0189】図5において、19, 20, 21はテキストデータ、コンピュータグラフィックス画面あるいはコンピュータプログラムであるバイナリデータ、音声データあるいは映像データが格納された第1, 第2及び第3のデータベース、4は1次ユーザ端末装置、5は2次ユーザ端末装置、6は3次ユーザ端末装置、7はn次ユーザ端末装置、10はデータ著作権を管理する著作権管理センタであり、8は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するCATV回線等である通信ネットワークである。

【0190】これらのうち第1, 第2及び第3データベース19, 20, 21, 著作権管理センタ10, 1次ユーザ端末装置4, 2次ユーザ端末装置5, 3次ユーザ端末装置6及びn次ユーザ端末装置7は通信ネットワーク8によって相互に接続可能とされている。

【0191】このシステムを利用する各ユーザは予め各々のデータベース組織に登録をしておく必要がある。また、この登録の際に各データベース組織の利用ソフトウェアがユーザに対して供給される。このソフトウェアにはデータ通信用プロトコル等の通常の通信用ソフトウェアプログラムが含まれている。これらのデータベース組織利用ソフトウェアは、ユーザ端末装置内の固定ディスクに格納してもよいが、ユーザ端末装置に内蔵されるマ

スクROM, EPROM, EEPROM等に格納することも可能である。

【0192】また、このシステムにおいてはユーザ側で秘密鍵を生成するためにユーザ端末装置に暗号鍵生成アルゴリズムが格納されるが、この暗号鍵生成アルゴリズム自身は必ずしも秘密のものではないため、各々のデータベース組織利用ソフトウェアに内蔵させてもよい。なお、広告付等の無料で供給される原データの場合には、暗号化を必要としない場合もあるが、その場合でも著作権は存在するため著作権を使用するための手続きは必要である。この図において、破線で示された経路は暗号化されたデータの経路であり、実線で示された経路は各ユーザ端末装置から各データベース及び著作権管理センタへ要求を行う経路であり、1点鎖線で示された経路は各データベース及び著作権管理センタから各ユーザ端末装置へ利用形態に対応する許可情報、著作権管理プログラム及び暗号鍵が転送される経路である。

【0193】この実施例においては原データ毎に異なる秘密鍵及び著作権管理プログラムが使用されるが、これらは予め各データベース及び著作権管理センタに保管されている。

【0194】第1データベース19には、第1原データM1が暗号化されていない状態で保管されており、1次ユーザが1次ユーザ端末装置4を利用して第1データベース19にアクセスすると、データメニューが転送される。

【0195】データメニューが転送されると1次ユーザはデータメニュー検索を行い第1原データM1を選択し、1次ユーザ端末装置4を利用して、通信ネットワーク8を経由して第1データベース19に対して、原データ名あるいは原データ番号を指定して第1原データM1の供給を申し込むがこのときに1次ユーザ情報Iu1を提示する。

【0196】1次ユーザから第1原データM1の利用申し込みを受けた第1データベース19は、利用申込を受けた第1の原データM1を第1秘密鍵Ks1を用いて暗号化し、

$$Cm1ks1 = E(Ks1, M1)$$

1次ユーザ端末装置4に供給する。

【0197】第2データベース20には、第2原データM2が暗号化されていない状態で保管されており、1次ユーザが1次ユーザ端末装置4を利用して第2データベース20にアクセスすると、データメニューが転送される。

【0198】データメニューが転送されると1次ユーザはデータメニュー検索を行い第2原データM2を選択し、1次ユーザ端末装置4を利用して、通信ネットワーク8を経由して第2データベース20に対して、原データ名あるいは原データ番号を指定して第2原データM2の供給を申し込むがこのときに1次ユーザ情報Iu1を提

示する。

【0199】1次ユーザから第2原データM2の利用申し込みを受けた第2データベース20は、利用申込を受けた第2原データM2を第2秘密鍵Ks2を用いて暗号化し、

$$Cm2ks2 = E(Ks2, M2)$$

1次ユーザ端末装置4に供給する。

【0200】第3データベース21には、第2原データM3が暗号化されていない状態で保管されており、1次ユーザが1次ユーザ端末装置4を利用して第3データベース21にアクセスすると、データメニューが転送される。

【0201】データメニューが転送されると1次ユーザはデータメニュー検索を行い第3原データM3を選択し、1次ユーザ端末装置4を利用して、通信ネットワーク8を経由して第3データベース22に対して、原データ名あるいは原データ番号を指定して第3原データM3の供給を申し込むがこのときに1次ユーザ情報Iu1を提示する。

【0202】1次ユーザから第3原データM3の利用申し込みを受けた第3データベース21は、利用申込を受けた第3原データM3を第3秘密鍵Ks3を用いて暗号化し、

$$Cm3ks3 = E(Ks3, M3)$$

1次ユーザ端末装置4に供給する。

【0203】暗号化第1, 第2, 第3原データCm1ks1, Cm2ks2, Cm3ks3を供給された1次ユーザは、1次ユーザ端末装置4を利用して暗号化第1, 第2, 第3の原データCm1ks1, Cm2ks2, Cm3ks3を1次利用するために通信ネットワーク8を経由して、原データ名あるいは原データ番号を指定して、著作権管理センタ10に対して1次利用申込を行う。

【0204】1次ユーザからの暗号化第1, 第2, 第3原データCm1ks1, Cm2ks2, Cm3ks3の1次利用申し込みを受けた著作権管理センタ10は、第1原データM1の暗号鍵である第1秘密鍵Ks1とともに第1著作権管理プログラムP1, 第2原データM2の暗号鍵である第2秘密鍵Ks2とともに第2著作権管理プログラムP2, 第3原データM3の暗号鍵である第3秘密鍵Ks3とともに第3著作権管理プログラムP3を1次ユーザ端末装置4に供給する。

【0205】これらの著作権管理プログラムP1, P2, P3には暗号アルゴリズムを有する暗号プログラムが各々含まれており、これらの暗号プログラムにより新しい秘密鍵の生成及びデータの復号/暗号化が行われる。なお、これらの暗号アルゴリズムを各々第1, 第2, 第3秘密鍵Ks1, Ks2, Ks3に依存するものにしておけば、第1, 第2, 第3著作権管理プログラムP1, P2, P3を各第1, 第2, 第3原データM1, M2, M3に固有のものとするができる。



【0206】第1, 第2, 第3の秘密鍵Ks1, Ks2, Ks3を受け取った1次ユーザ端末装置4は、これらの秘密鍵を用いて暗号化された第1, 第2, 第3の各原データCm1ks1, Cm2ks2, Cm3ks3を復号化して、

$$M1 = D(Ks1, Cm1ks1)$$

$$M2 = D(Ks2, Cm2ks2)$$

$$M3 = D(Ks3, Cm3ks3)$$

復号化された各原データM1, M2, M3をそのままあるいは加工して利用する。また、第1著作権管理プログラムP1が第1秘密鍵Ks1に基づいて第4の秘密鍵Ks4を、第2著作権管理プログラムP2が第2秘密鍵Ks2に基づいて第5秘密鍵Ks5を、第3著作権管理プログラムP3が第3の秘密鍵Ks3に基づいて第6秘密鍵Ks6を、各々生成する。

$$Ks4 = P1(Ks1)$$

$$Ks5 = P2(Ks2)$$

$$Ks6 = P3(Ks3)$$

【0207】各原データM1, M2, M3あるいは加工データM4, M5, M6が1次ユーザ端末装置4内に保存される場合、記録媒体11に複写される場合、通信ネットワーク8を経由して2次ユーザ端末装置5に転送される場合には、第1の原データM1あるいは加工データM4が第1著作権管理プログラムP1により第4秘密鍵Ks4を用いて、第2の原データM2あるいは加工データM5が第2著作権管理プログラムP2により第5秘密鍵Ks5を用いて、第3の原データM3あるいは加工データM6が第3著作権管理プログラムP3により第6秘密鍵Ks6を用いて、各々暗号化される。

$$Cm1ks4 = E(Ks4, M1)$$

$$Cm2ks5 = E(Ks5, M2)$$

$$Cm3ks6 = E(Ks6, M3)$$

$$Cm4ks4 = E(Ks4, M4)$$

$$Cm5ks5 = E(Ks5, M5)$$

$$Cm6ks6 = E(Ks6, M6)$$

【0208】第4, 第5, 第6秘密鍵Ks4, Ks5, Ks6によって暗号化された原データCm1ks4, Cm2ks5, Cm3ks6あるいは暗号化された加工データCm4ks4, Cm5ks5, Cm6ks6は第1, 第2, 第3の原データ名あるいは原データ番号及び1次ユーザデータIu1とともに、記録媒体11に複写されて、あるいは通信ネットワーク8を経由して2次ユーザ端末装置5に転送される。

【0209】暗号化された第1, 第2, 第3の原データCm1ks4, Cm2ks5, Cm3ks6あるいは暗号化された加工データCm4ks4, Cm5ks5, Cm6ks6を供給された2次ユーザ端末装置5においては、原データ名あるいは原データ番号を指定することにより、第1, 第2, 第3の原データM1, M2, M3あるいは加工データMの2次利用を著作権管理センタ10に申し込む。

【0210】2次ユーザ端末装置5から第1, 第2, 第3の原データM1, M2, M3あるいは加工データM4, M

5, M6の2次利用申込を受けた著作権管理センタ10は、第1の原データ名から第1秘密鍵Ks1及び第1著作権管理プログラムP1を探し出し、第2の原データ名あるいは原データ番号から第2秘密鍵Ks2及び第2著作権管理プログラムP2を探し出し、第3の原データ名から第3秘密鍵Ks3及び第3著作権管理プログラムP3を探し出し、第1著作権管理プログラムP1が第1秘密鍵Ks1から第4秘密鍵Ks4を生成し、第2著作権管理プログラムP2が第2秘密鍵Ks2から第5秘密鍵Ks5を生成し、第3著作権管理プログラムP3が第3秘密鍵から第6の秘密鍵Ks6を生成し、

$$Ks4 = P1(Ks1)$$

$$Ks5 = P2(Ks2)$$

$$Ks6 = P3(Ks3)$$

第1, 第2, 第3の著作権管理プログラムP1, P2, P3とともに2次ユーザ端末装置5に供給する。

【0211】第4, 第5, 第6秘密鍵Ks4, Ks5, Ks6と第1, 第2, 第3著作権管理プログラムP1, P2, P3を受け取った2次ユーザ端末装置5では、暗号化された第1の原データCm1ks4あるいは加工データCm4ks4が第1著作権管理プログラムP1により第4秘密鍵Ks4を用いて、暗号化された第2の原データCm2ks5あるいは加工データCm5ks5が第2著作権管理プログラムP2により第5秘密鍵Ks5を用いて、暗号化された第3の原データCm3ks6あるいは加工データCm6ks6が第3著作権管理プログラムP3により第6秘密鍵Ks6を用いて、各々復号化され、

$$M4 = D(Ks4, Cm4ks4)$$

$$M5 = D(Ks5, Cm5ks5)$$

$$M6 = D(Ks6, Cm6ks6)$$

復号化された各データM4, M5, M6をそのままあるいは加工して利用する。

【0212】第1, 第2, 第3の原データM1, M2, M3あるいは加工データM4, M5, M6が2次ユーザ端末装置5内に保存される場合、記録媒体12に複写される場合、通信ネットワーク8を経由して2次ユーザ端末装置6に転送される場合には、第1の原データM1あるいは加工データM4は第1著作権管理プログラムP1により第4秘密鍵Ks4を用いて、第2の原データM2あるいは加工データM5は第2著作権管理プログラムP2により第5秘密鍵Ks5を用いて、第3の原データM3あるいは加工データM6は第3著作権管理プログラムP3により第6秘密鍵Ks6を用いて、各々暗号化される。

【0213】なお、この場合第1著作権管理プログラムP1が第4秘密鍵Ks4に基づいて第7秘密鍵Ks7を、第2著作権管理プログラムP2が第5秘密鍵Ks5に基づいて第8秘密鍵Ks8を、第3著作権管理プログラムP3が第6秘密鍵Ks6に基づいて第9秘密鍵Ks9を各々生成するようにし、

$$Ks7 = P1(Ks4)$$

$Ks8 = P2 (Ks5)$

$Ks9 = P3 (Ks6)$

これら第1, 第2, 第3の原データM1, M2, M3あるいは加工データM4, M5, M6が2次ユーザ端末装置5内に保存される場合、記録媒体12に複写される場合、通信ネットワーク8を経由して3次ユーザ端末装置6に転送される場合には、それら第1, 第2, 第3の原データM1, M2, M3あるいは加工データM4, M5, M6は第1, 第2, 第3著作権管理プログラムP1, P2, P3により第7, 第8, 第9秘密鍵Ks7, Ks8, Ks9を用いて暗号化されるようにすることもできる。

$Cm1ks7 = E (Ks7, M1)$

$Cm2ks8 = E (Ks8, M2)$

$Cm3ks9 = E (Ks9, M3)$

$Cm4ks7 = E (Ks7, M4)$

$Cm5ks8 = E (Ks8, M5)$

$Cm6ks9 = E (Ks9, M6)$

【0214】〔実施例13〕次に説明する実施例13は、実施例12と同様に複数のデータベースからユーザの要求に応じて供給される複数の原データを利用して新しいデータを作成する実施例であり、この実施例においては暗号鍵方式として秘密鍵方式が採用される。また、暗号化／復号化に用いられる暗号鍵の生成に実施例7及び実施例11の場合と同様にさらに著作権管理プログラムの使用回数が利用される。

【0215】この実施例においては、著作権管理プログラムにはカウンタが付属しており、このカウンタがプログラムの使用回数あるいは原データの利用回数を計数し、そのカウンタ数Nを利用して第4, 第5, 第6秘密鍵Ks4, Ks5, Ks6が生成される。2次ユーザは各々の原データの原データ名あるいは原データ番号、1次ユーザデータとともにカウンタ数Nを提示して、データの2次利用を著作権管理センタ10に申し込む。データの2次利用申込を受けた著作権管理センタ10は、各々の原データ名あるいは原データ番号から第1, 第2, 第3秘密鍵Ks1, Ks2, Ks3を探し出し、第1, 第2, 第3著作権管理プログラムP1, P2, P3により各々のデータの第1, 第2, 第3秘密鍵Ks1, Ks2, Ks3、1次ユーザIu1及び第1, 第2, 第3カウンタ数N1, N2, N3から第4, 第5, 第6秘密鍵Ks4, Ks5, Ks6を生成し、第4, 第5, 第6著作権管理プログラムP1, P2, P3とともに2次ユーザに提供する。これ以外の点は、実施例12のシステム構成と異なる点はないので具体的な説明は省略する。

【0216】〔実施例14〕1次ユーザが入手した原データをそのまま複写して2次ユーザに供給した場合にはそのデータに何等の価値も加えられていないため、そのデータに1次ユーザの著作権は発生しない。しかし、入手した原データから新しいデータを作成した場合、すなわち、入手した単一の原データから新しいデータを作成

した場合及び入手した複数の原データから新しいデータを作成した場合には、新しいデータについて1次ユーザの2次的著作権が発生する。

【0217】一方、加工に利用された原データにも著作権者の著作権が存在しているため、加工データには原データの著作権者の著作権と加工を行った1次ユーザの2次的著作権とが存在することになる。著作権は単なる物権ではなく人格権の要素が強い権利であるため、著作権者がその存在を強く主張することが多い。そのため、原データの加工が行われた場合であっても、加工データから原データあるいは著作権者を容易に特定できるようにすることが望ましい。

【0218】これまでに実施例1～13で説明したデータ著作権管理システムでは、原データあるいは加工データを暗号化することによってデータの著作権を管理しているが、このシステムではデータが原データであるのかあるいは加工データであるのか、また、加工データの中でどの部分が原データであり、どの部分が加工データであるのかが区別されることなくデータの著作権が管理されるため、加工データから原データあるいは著作権者を特定することはできない。

【0219】これから説明する実施例14ではデータを著作権しか存在しない原データと著作権に加えて2次的著作権も存在する加工データを区別できるとともに、著作権と2次的著作権を明確に管理することができる。

【0220】データの加工は加工用プログラムを利用して原データに改変を加えることによってなされるため、原データと加工内容（必要な場合はさらに加工用プログラム）が特定されることによって加工データが再現される。いいかえれば、原データと加工内容（必要な場合はさらに加工用プログラム）が特定されなければ加工データの再現は不可能である。実施例14で説明する2次的著作権の管理は、原データと加工内容（必要な場合はさらに加工用プログラム）を特定し、これらを管理することによって行われる。

【0221】単一の原データにより新しいデータを作成する場合には、原データAを改変して加工データ

「A'」を得る場合、原データAに1次ユーザがデータXを付加することにより加工データ「A+X」を得る場合、原データAを原データ要素A1, A2, A3・・・に分割し配列をA3, A2, A1のように変更して加工データ「A'」を得る場合、原データAを原データ要素A1, A2, A3・・・に分割し1次ユーザのデータXをX1, X2, X3・・・に分割しこれらを配列して加工データ「A1+X1+A2+X2+A3+X3・・・」を得る場合等がある。これらの場合、原データの改変、原データの配列変更、原データと1次ユーザデータの組み合わせ、原データの分割及び1次ユーザデータとの組み合わせ、が各々2次的著作権の対象となり、これらの2次的著作権

権を保護する必要がある。なお、1次ユーザが付加したデータXには1次ユーザの著作権が存在することはいうまでもない。

【0222】複数の原データを組み合わせることにより新しいデータを作成する場合には、原データA, B, C...を単純に組み合わせ加工データ「A+B+C...」を得る場合、原データA, B, C...に1次ユーザが付加したデータXを付加することにより加工データ「A+X」を得る場合、原データA, B, C...を原データ要素A1, A2, A3..., B1, B2, B3..., C1, C2, C3...に分割し組み合わせ配列を変更し加工データ「A1+B1+C1+...+A2+B2+C2+...+A3+B3+C3+...」を得る場合、原データA, B, C...を原データ要素A1, A2, A3..., B1, B2, B3..., C1, C2, C3...に分割し1次ユーザのデータX1, X2, X3...を組み合わせ配列を変更して加工データ「A1+B1+C1+X1+...+A2+B2+C2+X2+...+A3+B3+C3+X3+...」を得る場合等がある。これらの場合も、複数の原データの組み合わせ、複数の原データと1次ユーザデータの組み合わせ、複数の原データの分割及び配列変更、分割された複数の原データと1次ユーザデータの組み合わせ、が各々2次的著作権の対象となり、これらの2次的著作権を保護する必要がある。また、1次ユーザが付加したデータX1, X2, X3...には1次ユーザの著作権が存在することはいうまでもない。

【0223】図6に示されたのは複数の原データA, B, Cを利用して新しいデータDを作成する手法例である。この手法は原データA, B, Cから要素a, b, cを抽出(カット)し、抽出された要素a, b, cを貼り付けて(ペースト)1つのデータDを合成するカットアンドペースト手法によってデータの加工を行うものである。

【0224】ところで、原データ及び1次ユーザデータがデータであることは明白であるが、データの加工過程である原データの改変、原データの配列変更、原データと1次ユーザデータの組み合わせ、原データの分割及び1次ユーザデータとの組み合わせ、複数の原データの組み合わせ、複数の原データと1次ユーザデータの組み合わせ、複数の原データの分割及び配列変更、分割された

複数の原データと1次ユーザデータの組み合わせもデータそのものである。

【0225】これまでに説明した実施例1～13では、データの著作権を原データあるいは加工データを暗号化することによってデータそのものの著作権を管理しているがこの他に、原データの配置関係及び加工手順等であるデータの加工過程もデータであることに着目すると、加工データに関する2次的著作権を原データに関する原著者の1次著作権及び1次ユーザデータに関する1次ユーザの1次著作権に加えて加工過程データに関する1

次ユーザの1次著作権を管理することによって保護することが可能となる。なお、加工過程や加工用プログラムを加工シナリオと呼ぶこともできる。

【0226】すなわち、加工データを原データと1次ユーザデータと加工過程データとから構成するものとし、これらの原データ、1次ユーザデータ及び加工過程データを各々これまでに実施例1～13で説明したデータ著作権管理システムによって管理することにより、原データとともに加工データの著作権を充分に管理することができる。なお、この場合データの加工において使用された加工用プログラムも必要ならばデータ著作権管理システムの管理対象とする。

【0227】このデータの加工は原データをその原データに対応する加工プログラムを使用して加工することもできるが、原データを最近注目されているオブジェクト指向ソフトウェアとして取り扱うようにすれば、より容易な加工とよりよいデータ著作権管理を行うことができる。また、さらに進んでエージェント指向ソフトウェアを採用すれば、ユーザは労することなくデータの合成を行うことができる。

【0228】エージェント指向ソフトウェアは、自律性・適応性・協調性を兼ね備えたプログラムであり、従来のソフトウェアのようにすべての作業手順を具体的に指示しなくても、ユーザの一般的な指示のみに基づいてその自律性・適応性・協調性との特質により、ユーザの要求に応えることができる。このエージェントプログラムをデータ著作権管理システムの基本的なシステムの中に組み込み、ユーザのデータベース利用形態を監視させ、その結果得られた情報をデータベース側あるいは著作権管理センタ側で収集するように構成することにより、ユーザのデータベース利用傾向をデータベース側あるいは著作権管理センタ側が知ることができ、よりきめの細かい著作権管理を行うことができる。したがって、エージェントプログラム及びデータも著作権保護の対象となり、原データと同様に暗号化される。

【0229】〔実施例15〕著作物中には、著作権が存在しないものと著作権が存在するものとがあり、著作権が存在するものの中には、著作権の行使が行われるものと著作権の行使が行われないものがある。著作権が存在しない著作物としては法令によって著作権が存在しないものとされている著作物と著作権の期限が過ぎてしまったものがある。これらの著作権が存在しない著作物を除くすべての著作物には著作権が存在するが、著作権が存在する著作物には通常著作権の存在を主張する表示がなされており、この表示があることによって著作権の侵害に対する抑止効果が発揮される。このことは、著作物がデータである場合にも同様であって、著作権が存在するデータの場合には利用されるデータあるいはデータのファイルヘッダに著作権表示あるいは著作権者表示が行われることによってデータ著作権の侵害行為が抑止され



る。また、データに著作権が存在することを示す著作権フラグをファイルに付加し、ユーザ端末装置においてこのフラグを識別するようにすることにより、データ著作権の侵害行為を阻止することができる。

【0230】しかしながら、このような著作権に関する表示がなされていたとしてもそのデータ著作物を利用するユーザが著作権の存在を無視した場合には著作権の侵害が行われる可能性がある。そのような場合に対処するために、これまで説明した実施例においてはデータを暗号化し、暗号化データを復号化するための復号鍵を管理し、復号化データが保存、複写、転送される場合には復号鍵とは異なる暗号鍵を用いて暗号化／復号化が行われる。そのような場合であっても、ユーザ端末装置の主記憶装置上にデータが存在している状態においてデータをユーザ端末装置の主記憶装置以外の記憶装置に転送することにより、復号鍵と異なる暗号鍵を用いることなくデータを保存、複写、転送する可能性を完全に否定することはできない。

【0231】このような事態を防止するには、データ著作権利用ソフトウェアをユーザ端末装置の基本システムに組み込み、著作権行使の対象であるデータ著作物のファイルには著作権行使の属性を表示し、データ著作物の著作権行使属性についてユーザ端末装置の基本システムが監視し、著作権行使属性を有するデータ著作物はデータ著作権利用ソフトウェアによって管理されるようにすることが最善である。基本システムとしては、ユーザ端末装置がパーソナルコンピュータ等のコンピュータである場合にはDOS等のソフトウェアオペレーティングシステムであり、ユーザ端末装置が携帯情報端末装置あるいはSTB（セットトップボックス）である場合にはROMに内蔵されたハードウェアオペレーティングシステムである。なお、このオペレーティングシステムによるデータ著作権管理をより強固なものとするためには、データ著作権利用ソフトウェアはオペレーティングシステムのできるだけ上位のレベルに組み込むことが望ましい。

【0232】ユーザ端末装置の内部における処理及びデータはすべてオペレーティングシステムの管理下におかれている。言い換えれば、オペレーティングシステムはユーザ端末装置の内部における処理及びデータをすべて把握することができる。したがって、ユーザの指示によるのではなくオペレーティングシステムが把握したデータの利用状況に応じて著作権管理プログラムが自動的にデータ著作権の管理を行うようにすることができ、このような構成によればユーザによるデータ著作権の利用が容易になるとともに、より完全なデータ著作権管理を行うことができる。また、暗号鍵、データ著作権情報あるいは著作権ラベル等を管理する著作権管理プログラムはオペレーティングシステム自体が管理するシステム領域

きないシステム領域に保持されることが望ましい。

【0233】しかし、この場合でもデータ著作物の一部のみが切りとられて利用されたような場合にはデータ著作権の管理が著しく困難になる。したがって、そのような状況をオペレーティングシステムが認識した場合には著作権管理プログラムにより切りとられた一部のデータに原データが有していた著作権情報及び著作権行使属性を付与するように構成することにより、切りとられた一部のデータのデータ著作権も管理する事が可能となる。

また、切り取られたデータに元のデータ著作物の著作権を継承させるために、著作権管理プログラムによりその切り取られたデータと元のデータ著作物との間に親子関係のリンクを形成する。このようにしておけばユーザが複数の著作権付きデータからそれぞれ希望する部分を切り出して取り込み新しいデータを作成した場合にも、その新しいデータに元の各データ著作物の著作権を継承させることができる。

【0234】〔実施例16〕著作権は財産権の一種であるから、著作権を利用する場合には当然のこととして使用料支払いの問題が発生する。また、秘密鍵の提供、著作権管理プログラムの提供等のサービスは有料で行われる必要がある。これらの料金支払の最も簡易な方法は請求書の発行と支払を組み合わせたものであるが、この方法は使用料の支払が直接に行われる反面、作業が煩雑な上、不払い等の事故の可能性もある。また、通信回線事業者が行う料金徴収代行方法もあり、この方法は料金徴収作業を通信回線事業者が行うため簡便であり、不払い等の事故の可能性が低い反面、使用料の徴収が直接に行われないため、料金徴収代行手数料の支払が必要となる。

【0235】これらの問題を解決する方法として、デジタルキャッシュを利用する方法がある。このデジタルキャッシュはデジタルデータであり、暗号化され使用される。

【0236】〔実施例17〕さらに、以上説明したデータ著作権管理システムの構成はデータの流通だけではなくデジタルキャッシュの流通に対しても適用可能である。これまでに種々提案されているデジタルキャッシュシステムは秘密鍵方式で暗号化デジタルキャッシュデータを銀行預金口座あるいはクレジット会社のキャッシングサービスから転送してICカードに保存しており、入出力用の端末装置を利用して支払を行う。このICカードを電子財布として利用するデジタルキャッシュシステムは商店等入出力用の端末装置が設置されている場所であればどこでも使用可能である反面、入出力用の端末装置がない場所、例えば家庭等、では使用不可能である。

【0237】ところで、デジタルキャッシュは暗号化データであるからICカード以外にも暗号化データを保存することができ、かつ支払先にデータを転送すること

ができる装置であればどのようなものでもデジタルキャッシュデータを保存する電子財布として利用することができる。具体的に電子財布として利用可能なユーザ端末装置としては、パーソナルコンピュータ、インテリジェントテレビジョン装置、携帯情報端末装置 (Personal Digital Assistant PDA), PHS (Personal Handyphone System) 等の携帯電話器、インテリジェント電話機、入出力機能を有するPCカード等がある。

【0238】このような端末装置をデジタルキャッシュ用の電子財布として利用することによる取引は、これまでに説明したデータ著作権管理システムの構成におけるデータベース1を顧客側銀行に、1次ユーザ端末装置4を顧客に、2次ユーザ端末装置5を小売店に、著作権管理センタ18を小売店側銀行に、3次ユーザ端末装置6を卸売またはメーカに置き換えることにより実現される。

【0239】また、デジタルキャッシュは単なるデータではなくデータと機能が結びついたオブジェクト (object) として処理されることが望ましい。デジタルキャッシュの取り扱いにおいては共通のデジタルキャッシュフォーム、所有者固有の未記入デジタルキャッシュフォーム、所有者固有のデジタルキャッシュフォームの書き込み欄、金額であるデジタルキャッシュデータ、デジタルキャッシュ取り扱いの指示、金額が書き込まれた所有者固有のデジタルキャッシュフォームがある。一方、オブジェクト指向プログラミング (object-oriented programming) においては、オブジェクト、クラス (class)、スロット (slot)、メッセージ (message)、インスタンス (instance) との概念が使用される。これらの対応関係は、共通のデジタルキャッシュフォームがオブジェクトとなり、所有者固有の未記入デジタルキャッシュフォームがクラスとなり、所有者固有のデジタルキャッシュフォームの記入欄がスロットとなり、デジタルキャッシュ取り扱いの指示がメッセージとなり、金額が記入された所有者固有のデジタルキャッシュフォームがインスタンスとなる。金額等からなるデジタルキャッシュデータは引数 (argument) として使用され、メッセージによりインスタンス変数 (instance variable) とも呼ばれるスロットに引き渡されて格納されることにより、金額等が更新されたデジタルキャッシュである新しいインスタンスが作られる。

【0240】オブジェクト化されたデジタルキャッシュについて、図6を用いて具体的に説明する。この図において、23、25、27は顧客端末装置に保存されている金額が書き込まれた顧客固有のデジタルキャッシュフォーム、29は小売店端末装置に保存されている金額が記入された小売店固有のデジタルキャッシュフォーム、24、26、28は各々の顧客の取引銀行にある預金口座である。

【0241】顧客23はデジタルキャッシュを使用す

るために、預金口座24から必要な金額を引き出し、端末装置に保存されているデジタルキャッシュフォーム23にデジタルキャッシュ引出金データ31を引き渡す。この場合、デジタルキャッシュフォーム23にはデジタルキャッシュ残金データ30が既に記入されているのが普通であるため、デジタルキャッシュフォーム23はクラスではなくインスタンスである。デジタルキャッシュ引出金データ31はデジタルキャッシュ残金データ30に対して加算することを指示するメッセージによりデジタルキャッシュフォーム23の記入欄であるスロットに引数として引き渡され、デジタルキャッシュフォーム23のデジタルキャッシュ残金データ30にデジタルキャッシュ引出金データ31が加算されてデジタルキャッシュフォーム23の記入欄の金額が変更された新しいインスタンスが作られる。

【0242】顧客が小売店に対して支払を行う場合には、支払金額に相当するデジタルキャッシュ支払金データ32をデジタルキャッシュフォーム23の記入欄の金額から減算することを指示するメッセージによりデジタルキャッシュフォーム記入欄であるスロットに引数として引き渡され、デジタルキャッシュフォーム23のデジタルキャッシュ残金データ30及びデジタルキャッシュ引出金データ31からデジタルキャッシュ支払金データ32が減算されてデジタルキャッシュフォーム23の記入欄の金額が変更された新しいインスタンスが作られる。また、デジタルキャッシュ支払金データ32が小売店固有のデジタルキャッシュフォーム29に引き渡される。

【0243】同様な引出処理及び支払処理が他の顧客のデジタルキャッシュフォーム25及び27でも行われ、デジタルキャッシュフォーム25からはデジタルキャッシュ支払金データ33が、デジタルキャッシュフォーム27からはデジタルキャッシュ支払金データ34が小売店固有のデジタルキャッシュフォーム29に引き渡される。小売店固有のデジタルキャッシュフォーム29の場合にもデジタルキャッシュ残金データ35が既に記入されているのが普通である。デジタルキャッシュ支払金データ32、デジタルキャッシュ支払金データ33及びデジタルキャッシュ支払金データ34はデジタルキャッシュ残金データ35に対して加算することを指示するメッセージによりデジタルキャッシュフォーム29の記入欄であるスロットに引数として引き渡され、デジタルキャッシュ残金データ35にデジタルキャッシュ支払金データ32、デジタルキャッシュ支払金データ33及びデジタルキャッシュ支払金データ34が加算されて、デジタルキャッシュフォーム記入欄の金額が変更された新しいインスタンスが作られる。

【0244】通常のオブジェクト指向プログラミングにおいては、引数がメッセージによりスロットに引き渡さ



れることにより新しいインスタンスが作られ、新しく作られたインスタンス全体引き渡されることはない。しかし、デジタルキャッシュの場合には安全上暗号技術が使用されるから、支払元においてデジタルキャッシュ支払金データが記入されたインスタンスを作り、このインスタンスを暗号化して支払先に引き渡すこともできる。

【0245】デジタルキャッシュを通信ネットワークを経由して転送することにより行われる取引システムの実施例を図7を用いて説明する。この実施例は図4に示されたシステム構成を利用したものであり、この図において、36は顧客、37は顧客36の取引銀行、38は小売店、39は小売店38の取引銀行、40はメーカ、41はメーカ40の取引銀行、8は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するCATV回線等の通信ネットワークであり、顧客36、顧客の取引銀行37、小売店38、小売店の取引銀行39、メーカ40及びメーカの取引銀行41は通信ネットワーク8によって相互に接続可能とされている。このシステムにおいて、顧客36は銀行の他にキャッシングサービスを行うクレジット会社を利用することが可能であり、小売店とメーカとの間に適当な数の卸売り店を介在させることが可能である。また、42及び43はデジタルキャッシュデータが格納されるICカードあるいはPCカードであり、通信ネットワークを利用しない場合に使用される。なお、この図において、破線で示されたのは暗号化されたデジタルキャッシュデータの経路であり、実線で示されたのは顧客、小売店あるいはメーカから銀行への要求の経路であり、1点鎖線で示されたのは各銀行からの秘密鍵の経路である。さらに、この実施例では暗号鍵として顧客側銀行37が用意する第1秘密鍵及び顧客が生成する第2秘密鍵、小売店が生成する第3秘密鍵及びメーカが生成する第4秘密鍵が用いられる。この実施例では顧客側銀行37、小売店側銀行39、メーカ側銀行41を別個のものとして説明したが、これらを一括して金融システムとして考えてもよい。

【0246】デジタルキャッシュデータを暗号化/復号化するデジタルキャッシュ管理プログラムPは顧客36に予め配布され、ユーザ端末装置に保存されている。また、デジタルキャッシュ管理プログラムPは銀行との取引が行われる毎にデータとともに転送されるようにすることもできる。さらに、デジタルキャッシュ管理プログラムPは全銀行において共通するものとするのが望ましい。顧客36はユーザ端末装置を利用して通信ネットワーク8を経由して金額を指定することにより、顧客側銀行37に預金口座からの預金の引出の申込を行うがこのときに顧客36の顧客情報Icを提示する。

【0247】顧客36から預金引出の申込を受けた顧客

側銀行37は、第1秘密鍵Ks1を選択あるいは作成し、引出金額のデジタルキャッシュデータM0をこの第1秘密鍵Ks1で暗号化し、

$$Cm0ks1 = E(Ks1, M0)$$

暗号化デジタルキャッシュデータCm0ks1及び復号鍵である第1秘密鍵Ks1を顧客36に転送するとともに、顧客情報Ic及び第1秘密鍵Ks1を保管する。この場合、第1秘密鍵Ks1は顧客側銀行37が予め用意したものから選択してもよいが、顧客が引き出し時に顧客情報Icを提示し、デジタルキャッシュ管理プログラムPにより、提示された顧客情報Icに基づいて作成することもできる。

$$Ks1 = P(Ic)$$

このようにすれば、第1秘密鍵Ks1を顧客36に固有のものとするだけでなく、顧客36に対して第1秘密鍵Ks1を転送する必要がないため、システムの安全性が高くなる。また、第1秘密鍵Ks1は顧客側銀行37の銀行情報Ibsあるいは銀行情報Ibsと作成日時に基づいて作成することもできる。

【0248】暗号化デジタルキャッシュデータCm0ks1及び第1秘密鍵Ks1を転送された顧客36は、デジタルキャッシュ管理プログラムPにより、顧客情報Ic、第1秘密鍵Ks1の何れか1つあるいは双方に基づいて第2秘密鍵Ks2を生成し、

$$Ks2 = P(Ic)$$

生成された第2秘密鍵Ks2がユーザ端末装置内に保存される。また、顧客36はデジタルキャッシュ管理プログラムPにより暗号化デジタルキャッシュデータCm0ks1を第1秘密鍵Ks1を用いて復号化して

$$M0 = D(Ks1, Cm0ks1)$$

内容を確認するが、内容が確認された復号化デジタルキャッシュデータM0が電子財布であるユーザ端末装置内に保存される場合には、生成された第2秘密鍵Ks2を用いてデジタルキャッシュ管理プログラムPにより暗号化される。

$$Cm0ks2 = E(Ks2, M0)$$

また、このときに第1秘密鍵Ks1が廃棄される。

【0249】小売店38から物品の購入を希望する顧客36は、デジタルキャッシュ管理プログラムPにより電子財布であるユーザ端末装置に保存されている暗号化デジタルキャッシュデータCm0ks2を第2秘密鍵Ks2を用いて復号化し、

$$M0 = D(Ks2, Cm0ks2)$$

必要な金額に対応するデジタルキャッシュデータM1をデジタルキャッシュ管理プログラムPにより第2秘密鍵Ks2を用いて暗号化し、

$$Cm1ks2 = E(Ks2, M1)$$

通信ネットワーク8を介して暗号化デジタルキャッシュデータCm1ks2を小売店38の電子財布であるユーザ端末装置に転送することにより、支払を行う。このとき

に、顧客情報Icも小売店38のユーザ端末装置に転送される。また、残額デジタルキャッシュデータM2はデジタルキャッシュ管理プログラムPにより第2秘密鍵Ks2を用いて暗号化され、

$$Cm2ks2 = E(Ks2, M2)$$

顧客36のユーザ端末装置内に保存される。

【0250】暗号化デジタルキャッシュデータCmlks2及び顧客情報Icを転送された小売店38は、転送された暗号化デジタルキャッシュデータCmlks2及び顧客情報Icをユーザ端末装置に保存するとともに、内容を確認するために通信ネットワーク8を経由して小売店側銀行39に顧客情報Icを提示して、復号鍵である第2秘密鍵Ks2の転送を依頼する。小売店38から第2秘密鍵Ks2の転送依頼を受けた小売店側銀行39は、第2秘密鍵Ks2の転送依頼とともに顧客情報Icを顧客側銀行37に転送する。小売店側銀行39から第2秘密鍵Ks2の転送依頼を転送された顧客側銀行37は、第2秘密鍵Ks2が顧客情報Icのみに基づいている場合にはデジタルキャッシュ管理プログラムPにより顧客情報Icに基づいて第2秘密鍵Ks2を生成し、第2秘密鍵Ks2が顧客情報Icと第1秘密鍵Ks1に基づいている場合にはデジタルキャッシュ管理プログラムPにより顧客情報Icと第1秘密鍵Ks1に基づいて第2秘密鍵Ks2を生成し、生成された第2秘密鍵Ks2を小売店側銀行39に転送する。顧客側銀行37から第2秘密鍵Ks2を転送された小売店側銀行39は、通信ネットワーク8を経由して第2秘密鍵Ks2を小売店38に転送する。

【0251】第2秘密鍵Ks2を転送された小売店38は、デジタルキャッシュ管理プログラムPにより第2秘密鍵Ks2を用いて暗号化デジタルキャッシュデータCmlks2を復号化し、

$$M1 = D(Ks2, Cmlks2)$$

金額を確認の上、商品を顧客36に発送する。なお、この場合小売店36が小売店側銀行39ではなく顧客側銀行37に直接に第2秘密鍵Ks2の転送を依頼するようにすることもできる。

【0252】小売店38が収受したデジタルキャッシュを小売店側銀行39の口座に入金する場合には、通信ネットワーク8を経由して小売店側銀行39に暗号化デジタルキャッシュデータCmlks2とともに顧客情報Icを転送する。暗号化デジタルキャッシュデータCmlks2と顧客情報Icを転送された小売店側銀行39は、顧客情報Icを転送することにより第2秘密鍵Ks2の転送を顧客側銀行24に対して依頼する。小売店側銀行39から第2秘密鍵Ks2の転送を依頼された顧客側銀行37は、第2秘密鍵Ks2が顧客情報Icのみに基づいている場合にはデジタルキャッシュ管理プログラムPにより顧客情報Icに基づいて第2秘密鍵Ks2を生成し、第2秘密鍵Ks2が顧客情報Icと第1秘密鍵Ks1に基づいている場合にはデジタルキャッシュ管理プログラムPに

より顧客情報Icと第1秘密鍵Ks1に基づいて第2秘密鍵Ks2を生成し、生成された第2秘密鍵Ks2を小売店側銀行39に転送する。顧客側銀行37から第2秘密鍵Ks2を転送された小売店側銀行39は、デジタルキャッシュ管理プログラムPにより第2秘密鍵Ks2を用いて暗号化デジタルキャッシュデータCmlks2を復号化し、

$$M1 = D(Ks2, Cmlks2)$$

復号化デジタルキャッシュデータM1を小売店39の銀行口座に入金する。

【0253】一般的な取引システムにおいては、小売店38はメーカ40あるいはメーカ40と小売店38の間に介在する卸売り店から商品を仕入れ、顧客36に販売する。そのため、顧客36と小売店38との間に存在するのと同様の取引形態が小売店38とメーカ40の間にも存在する。この小売店38とメーカ40の間で行われるデジタルキャッシュの取扱いは、顧客36と小売店38との間で行われるデジタルキャッシュの取扱いと基本的な相違はないため、煩雑さをさけるため説明を省略する。

【0254】このデジタルキャッシュシステムにおける、デジタルキャッシュの取扱いはすべて銀行を介在させて行われるため、顧客側銀行にデジタルキャッシュの取扱いに関する金額、日付、秘密鍵要求者情報等の情報を保存しておくことにより、デジタルキャッシュの残高及び使用履歴を把握することができる。また、デジタルキャッシュデータを保存する電子財布であるユーザ端末装置が紛失あるいは破損により使用不能となった場合でも、顧客側銀行に保存されている使用残高及び使用履歴に基づきデジタルキャッシュを再発行することが可能である。なお、デジタルキャッシュの安全性を高めるためにデジタルキャッシュデータにデジタル署名を付けることが望ましい。この実施例において、デジタルキャッシュには顧客情報が付加されており、この顧客情報はデジタル署名付とされることがある。つまり、この実施例においてデジタルキャッシュは顧客を振り出し人とする手形決済システムとしての機能も有する。さらに、このシステムは従来紙を用いて行われている国際貿易における信用状、船積み有価証券等による各種決済システムにも応用することができる。

【0255】〔実施例18〕実施例17で説明したデジタルキャッシュシステムにおけるデジタルキャッシュの取扱いはすべて銀行を介在させて行われるが、この他に銀行を介在させることなくデジタルキャッシュを取り扱うこともできるので、次に、銀行を介在させないデジタルキャッシュシステムを説明する。このデジタルキャッシュシステムにおいては、デジタルキャッシュデータを暗号化する暗号鍵として公開鍵及び専用鍵が用いられ、実施例17で用いられる秘密鍵Ks及び顧客情報Icは用いられない。したがって、この実施例においてデジタルキャッシュは貨幣と同様な形態で使用

される。これら以外の点は、実施例17のシステム構成と異なる点はないので具体的な説明は省略する。

【0256】このデジタルキャッシュシステムに関係する各銀行、顧客、小売店、メーカでデジタルキャッシュを受け取る側になる者は、各々公開鍵及び専用鍵を用意する。その中の公開鍵は支払予定者に予め送付しておくことも、あるいは取引を行う前に支払者に送付することもできるが、ここでは支払予定者に予め配布されているものとして説明する。顧客36は端末装置を利用して通信ネットワーク8を経由して金額を指定することにより、顧客側銀行37に預金口座からの預金の引出の申込を行う。顧客36から預金引出の申込を受けた顧客側銀行37は、引出金額のデジタルキャッシュデータM0を予め送付されている顧客公開鍵Kbcを用いてデジタルキャッシュ管理プログラムPにより暗号化し、  
 $Cm0kbc = E(Kbc, M0)$

暗号化デジタルキャッシュデータCm0kbcを顧客36に転送する。

【0257】暗号化デジタルキャッシュデータCm0kbcを転送された顧客36は、デジタルキャッシュ管理プログラムPにより顧客公開鍵Kbcに対応する顧客専用鍵Kvcを用いて復号化し、  
 $M0 = D(Kvc, Cm0kbc)$

内容を確認し、端末装置内に残金額のデータM1がある場合には残金額のデータをM2 ( $=M0+M1$ ) に変更し、金額が変更されたデジタルキャッシュデータM2をデジタルキャッシュ管理プログラムPにより顧客公開鍵Kbcで暗号化して、  
 $Cm2kbc = E(Kbc, M2)$

端末装置内に保存する。

【0258】小売店38から物品の購入を希望する顧客36は、端末装置に保存されている暗号化デジタルキャッシュデータCm2kbcをデジタルキャッシュ管理プログラムPにより顧客専用鍵Kvcを用いて復号化し、  
 $M2 = D(Kvc, Cm2kbc)$

必要な金額に対応するデジタルキャッシュデータM3を予め送付されている小売店公開鍵Kbsを用いてデジタルキャッシュ管理プログラムPにより暗号化し、  
 $Cm3kbs = E(Kbs, M3)$

通信ネットワーク8を介して小売店38の端末装置に転送することにより、支払を行う。また、残額デジタルキャッシュデータM4 ( $=M2-M3$ ) はデジタルキャッシュ管理プログラムPにより顧客公開鍵Kbcで暗号化されて、  
 $Cm4kbc = E(Kbc, M4)$

端末装置内に保存される。

【0259】暗号化デジタルキャッシュデータCm3kbsを転送された小売店38は、デジタルキャッシュ管理プログラムPにより小売店公開鍵Kbsに対応する小売店専用鍵Kvsを用いて復号化し、

$M3 = D(Kvs, Cm3kbs)$

内容を確認し、端末装置内に残金額のデータM5がある場合には残金額のデータをM6 ( $=M5+M3$ ) に変更し、金額が変更されたデジタルキャッシュデータM6をデジタルキャッシュ管理プログラムPにより小売店公開鍵Kbsで暗号化して、  
 $Cm6kbs = E(Kbs, M6)$   
 端末装置内に保存する。

【0260】メーカ40に対する商品仕入代金の決済を行うおうとする小売店38も同様な方法で決済を行う。さらには、顧客36の顧客側銀行37への入金、小売店36の小売店側銀行39への入金、メーカ40のメーカ側銀行41への入金も同様な方法で行われる。

【0261】以上説明した実施例17及び実施例18においては、デジタルキャッシュシステムを実現するために図4を用いて説明されたデータ著作権管理システムの構成を応用し、さらに実施例17においては顧客情報を利用し、用いられる秘密鍵を変化させ、実施例18においては公開鍵及び専用鍵を用いている。しかし、デジタルキャッシュシステムを実現させるシステムの構成として、この他の著作権管理システムの構成すなわち、図1に示されたデータ著作権管理システム、図2に示されたデータ著作権管理システム、図3に示されたデータ著作権システム、図5に示されたデータ著作権システムの何れの構成も応用可能である。また、その場合に用いられる暗号鍵方式としては、変化しない秘密鍵、公開鍵と専用鍵、秘密鍵と公開鍵と専用鍵の組み合わせ、鍵の2重化、という実施例1から実施例13で説明した暗号鍵方式の何れもが応用可能である。

【0262】[実施例19] これまでは従来の音声電話器にテレビジョン映像を付加したものに過ぎなかったテレビジョン会議システムが、最近ではコンピュータシステムに組み込まれることにより音声あるいは映像の品質が向上したばかりでなく、コンピュータ上のデータも音声及び映像と同時に扱うことができるように進化している。このような中で、テレビジョン会議参加者以外の盗視聴による使用者のプライバシー侵害及びデータの漏洩に対するセキュリティは秘密鍵を用いた暗号化システムによって保護されている。しかし、テレビジョン会議参加者自身が入手する会議内容は復号化されたものであるため、テレビジョン会議参加者自身が会議内容を保存し、場合によっては加工を行い、さらにはテレビジョン会議参加者以外の者に配布する2次的な利用が行われた場合には他のテレビジョン会議参加者のプライバシー及びデータのセキュリティは全く無防備である。特に、伝送データの圧縮技術が発達する一方でデータ蓄積媒体の大容量化が進んだ結果テレビジョン会議の内容全てがデータ蓄積媒体に複写されたりあるいはネットワークを介して転送される恐れさえ現実のものとなりつつある。

【0263】この実施例はこのような状況に鑑みて、こ



れまでに説明したデータ著作権管理システムの構成をテレビジョン会議システムに応用することにより、テレビジョン会議参加者自身の2次的な利用による他のテレビジョン会議参加者のプライバシー及びデータのセキュリティ確保を行うものである。

【0264】このテレビジョン会議データ管理システムは、例えば図4に示されたデータ著作権管理システムの構成におけるデータベース1をテレビジョン会議第1参加者に、1次ユーザ端末装置4をテレビジョン会議第2参加者に、2次ユーザ端末装置5をテレビジョン会議非参加者に置き換えることにより実現することができる。この実施例を図9を用いて説明する。この図において、44はテレビジョン会議第1参加者、45はテレビジョン会議第2参加者、46はテレビジョン会議第3非参加者及び47はテレビジョン会議第4非参加者、8は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するCAテレビジョン回線等の通信ネットワークであり、テレビジョン会議第1参加者44とテレビジョン会議第2参加者45は通信ネットワーク8によって相互に接続可能とされている。また、テレビジョン会議第2参加者45とテレビジョン会議第3非参加者46、テレビジョン会議第3非参加者46とテレビジョン会議第4非参加者47は通信ネットワーク8で接続可能とされている。また、48はデータ記録媒体である。この図において、破線で示されたのは暗号化されたテレビジョン会議内容の経路であり、実線で示されたのはテレビジョン会議第3非参加者46及びテレビジョン会議第4非参加者47からテレビジョン会議第1参加者へ暗号鍵を要求する経路であり、1点鎖線で示されたのはテレビジョン会議第1参加者44からテレビジョン会議第2参加者45、テレビジョン会議第3非参加者46及びテレビジョン会議第4非参加者47へ暗号鍵が転送される経路である。なお、この実施例で説明するテレビジョン会議データ管理システムでは説明を簡明にするために、テレビジョン会議第1参加者44のプライバシー及びデータセキュリティの確保のみが行われる場合について説明するが、テレビジョン会議第2参加者45のプライバシー及びデータセキュリティの確保も行うことが可能であることはいうまでもない。

【0265】映像及び音声を含むテレビジョン会議第1参加者44のテレビジョン会議データを暗号化/復号化するテレビジョン会議管理プログラムPはテレビジョン会議第2参加者45、テレビジョン会議第3非参加者46及びテレビジョン会議第4非参加者47に予め配布され、各々の端末装置に内蔵されている。なお、テレビジョン会議データ管理プログラムPは暗号鍵が転送される毎に転送されるようにすることもできる。さらに、この実施例では暗号鍵としてテレビジョン会議第1参加者44が用意する第1秘密鍵及びテレビジョン会議第2参加者45が生成する第2秘密鍵、テレビジョン会議第3非

参加者46が生成する第3秘密鍵・・・が用いられる。

【0266】テレビジョン会議第1参加者44とテレビジョン会議第2参加者45は、各端末装置を利用し、通信ネットワーク8を経由して音声、映像、データ（これらを一括して「テレビジョン会議データ」と呼ぶ）を相互に転送することによりテレビジョン会議を行うが、テレビジョン会議を開始する前にテレビジョン会議第1参加者44は第1秘密鍵Ks1を選択あるいは生成し、第1秘密鍵Ks1をテレビジョン会議を開始する前にテレビジョン会議第2参加者45に供給する。また、第1秘密鍵Ks1を転送されたテレビジョン会議第2参加者45は、テレビジョン会議データ管理プログラムPにより、第1秘密鍵Ks1に基づいて第2秘密鍵Ks2を生成し、 $Ks2 = P(Ks1)$

生成された第2秘密鍵Ks2を端末装置内に保存しておく。

【0267】テレビジョン会議第1参加者44は、通信ネットワーク8を経由して行われるテレビジョン会議において、テレビジョン会議データM0を第1秘密鍵Ks1で暗号化し、

$$Cm0ks1 = E(Ks1, M0)$$

暗号化されたテレビジョン会議データCm0ks1をテレビジョン会議第2参加者45に転送する。

【0268】第1秘密鍵Ks1を用いて暗号化されたテレビジョン会議データCm0ks1を受け取ったテレビジョン会議第2参加者45は、第1秘密鍵Ks1を用いて暗号化テレビジョン会議データCm0ks1を復号し、 $M0 = D(Ks1, Cm0ks1)$

復号化されたテレビジョン会議データM0を利用する。

また、テレビジョン会議データ管理プログラムPにより、第1秘密鍵Ks1に基づいて第2秘密鍵Ks2が生成される。

$$Ks2 = P(Ks1)$$

【0269】復号されたテレビジョン会議データM0がテレビジョン会議第2参加者45の端末装置内に保存される場合、データ記録媒体48に複写される場合、通信ネットワーク8を経由してテレビジョン会議第3非参加者に転送される場合には、そのデータMはテレビジョン会議データ管理プログラムPにより第2秘密鍵Ks2を用いて暗号化される。

$$Cmks2 = E(Ks2, M)$$

【0270】暗号化データCmks2は、テレビジョン会議データ名あるいはテレビジョン会議データ番号とともに、記録媒体11に複写され、あるいは、通信ネットワーク8を経由してテレビジョン会議第3非参加者に供給される。

【0271】暗号化データCmks2を入手したテレビジョン会議第3非参加者46は端末装置を利用して、テレビジョン会議データ名あるいはテレビジョン会議データ番号を指定することによりテレビジョン会議データMの2

次利用をテレビジョン会議第1参加者44に申し込む。

【0272】データMの2次利用申込を受けたテレビジョン会議第1参加者44は、テレビジョン会議データ名あるいはテレビジョン会議データ番号を手がかりとして第1秘密鍵Ks1を探し出し、第1秘密鍵Ks1に基づいて第2秘密鍵Ks2を生成し、

$$Ks2 = P(Ks1)$$

生成された第2秘密鍵Ks2をテレビジョン会議第3非参加者46に供給する。

【0273】第2秘密鍵Ks2を受け取ったテレビジョン会議第3非参加者46は、暗号化データCmks2をテレビジョン会議データ管理プログラムPを利用して第2秘密鍵Ks2を用いて復号化して

$$M = D(Ks2, Cmks2)$$

復号化されたテレビジョン会議データMを利用する。テレビジョン会議データMがテレビジョン会議第3非参加者46の端末装置内に保存される場合、記録媒体49に複写される場合、通信ネットワーク8を経由してテレビジョン会議第4非参加者47に転送される場合には、そのテレビジョン会議データMはテレビジョン会議データ管理プログラムPにより第2秘密鍵Ks2を用いて暗号化される。

$$Cmks2 = E(Ks2, M)$$

【0274】なお、さらにテレビジョン会議データ管理プログラムPにより第2秘密鍵Ks2に基づいて第3秘密鍵Ks3が生成され、

$$Ks3 = P(Ks2)$$

テレビジョン会議データ管理プログラムPによりこの生成された第3秘密鍵Ks3を用いてデータMが暗号化されるようにすることもできる。

$$Cmks3 = E(Ks3, M)$$

【0275】以上説明した実施例19においては、テレビジョン会議データ管理システムを実現するために図4を用いて説明されたデータ著作権管理システムの構成を応用し、使用される秘密鍵を変化させている。しかし、テレビジョン会議データシステムを実現させるシステムの構成として、この他のシステム構成すなわち、図1に示されたシステム構成、図2に示されたシステム構成、図3に示されたシステム構成、図5に示されたシステム構成の何れもが応用可能である。また、その場合に用いられる暗号鍵方式としては、変化しない秘密鍵、公開鍵と専用鍵、秘密鍵と公開鍵と専用鍵の組み合わせ、鍵の2重化、という実施例1から実施例13で説明した暗号鍵方式が応用可能である。

【0276】また、この説明ではテレビジョン会議第2参加者がテレビジョン会議データを保存して利用すること及び記録媒体に複写あるいは通信ネットワークを経由して転送することを前提にしているが、暗号化に使用された暗号鍵が直ちに廃棄されるようにすることにより、

これらの行為を制限することもできる。

【0277】[実施例20]前に説明したように、本発明のシステムを利用する各ユーザは予めデータベース組織に登録をしておく必要があり、また、この登録の際にデータベース用ソフトウェアがユーザに対して提供される。このソフトウェアにはデータ通信用プロトコル等の通常の通信用ソフトウェアの他に第1暗号鍵を用いた著作権管理プログラムを復号するためのプログラムが含まれているため、その保護を図る必要がある。また、本発明においてはデータMを利用するために第1暗号鍵K1、第2暗号鍵K2及び著作権管理プログラムPが各ユーザに対して転送され、各ユーザはこれらを保管しておく必要がある。さらには著作権情報ラベル、ユーザ情報、公開鍵方式の公開鍵と専用鍵そして秘密鍵生成アルゴリズムを含むプログラム等が必要に応じて保管される。

【0278】これらを保管しておく手段としてフレキシブルディスクを使用することが最も簡便な手段であるが、フレキシブルディスクはデータの消失あるいは改竄に対して極めて脆弱である。また、ハードディスクドライブを使用した場合にもフレキシブルディスク程ではないがデータの消失あるいは改竄に対する不安がある。ところで、最近カード形状の容器にIC素子を封入したICカードが普及し、特にマイクロプロセッサを封入したPCカードがPCMCIAカードあるいはJEIDAカードとして規格化が進められている。

【0279】図10に示されたのは、このPCカードを用いて本発明のデータベース著作権管理システムのユーザ端末装置を構成した実施例である。この図において、50はユーザ端末装置本体のマイクロプロセッサであり、51はシステムバスである。また、52は内部にPCカードマイクロプロセッサ53、読み出し専用メモリ55、書き込み・読み出しメモリ56が封入されこれらがPCカードマイクロプロセッサバス54で接続されたPCカードである。

【0280】読み出し専用メモリ55には、データベース用ソフトウェア及びユーザデータ等の固定した情報がデータベース組織において格納されている。また、この読み出し専用メモリ55には鍵管理センタ9あるいは著作権管理センタから供給される第1暗号鍵、第2暗号鍵及び著作権管理プログラムも格納される。この読み出し専用メモリ55は書き込みも行われるため、EEPROMを使用することが最も簡便である。

【0281】前に説明したように、データ、第1暗号鍵K1、第2暗号鍵K2、第3暗号鍵K3・・・及び著作権管理プログラムP1、P2、P3・・・はいずれも暗号化された状態でユーザに供給され、データを利用するには第1暗号鍵K1、著作権管理プログラムP、データM及び第2暗号鍵K2を復号しなければならない。これらの作業はユーザ端末装置本体のマイクロプロセッサ50がPCカード52の読み出し専用メモリ55に格納され



ているソフトウェア、第1暗号鍵K1及び著作権管理プログラムP1を用いて行ってもよいが、その場合にはこれらのデータがユーザ端末装置に転送されるため、不正規な使用が行われる危険性がある。この危険を避けるためにはすべての作業をPCカード52内のマイクロプロセッサ53がCPUバス54を介して書き込み・読み出しメモリ56を利用して行い、結果だけをユーザ端末装置に転送し各種の利用を行うようにする。このPCカードを利用した場合には異なる装置をユーザ端末装置とすることができる。また、PCカードの他にこれらの機能を有するボードあるいは外部装置を用いることもできる。

#### 【図面の簡単な説明】

【図1】 本発明実施例1、実施例2、実施例3のデータ著作権管理システム構成図。

【図2】 本発明実施例4のデータ著作権管理システム構成図。

【図3】 本発明実施例5、実施例6、実施例7のデータ著作権管理システム構成図。

【図4】 本発明実施例8、実施例9、実施例10、実施例11のデータ著作権管理システム構成図。

【図5】 本発明実施例12、実施例13のデータ著作権管理システムの実施例。

【図6】 データ加工の説明図。

【図7】 デジタルキャッシュシステムの説明図。

【図8】 本発明実施例17、実施例18のデジタルキャッシュシステム構成図。

【図9】 本発明実施例19のテレビジョン会議システム構成図。

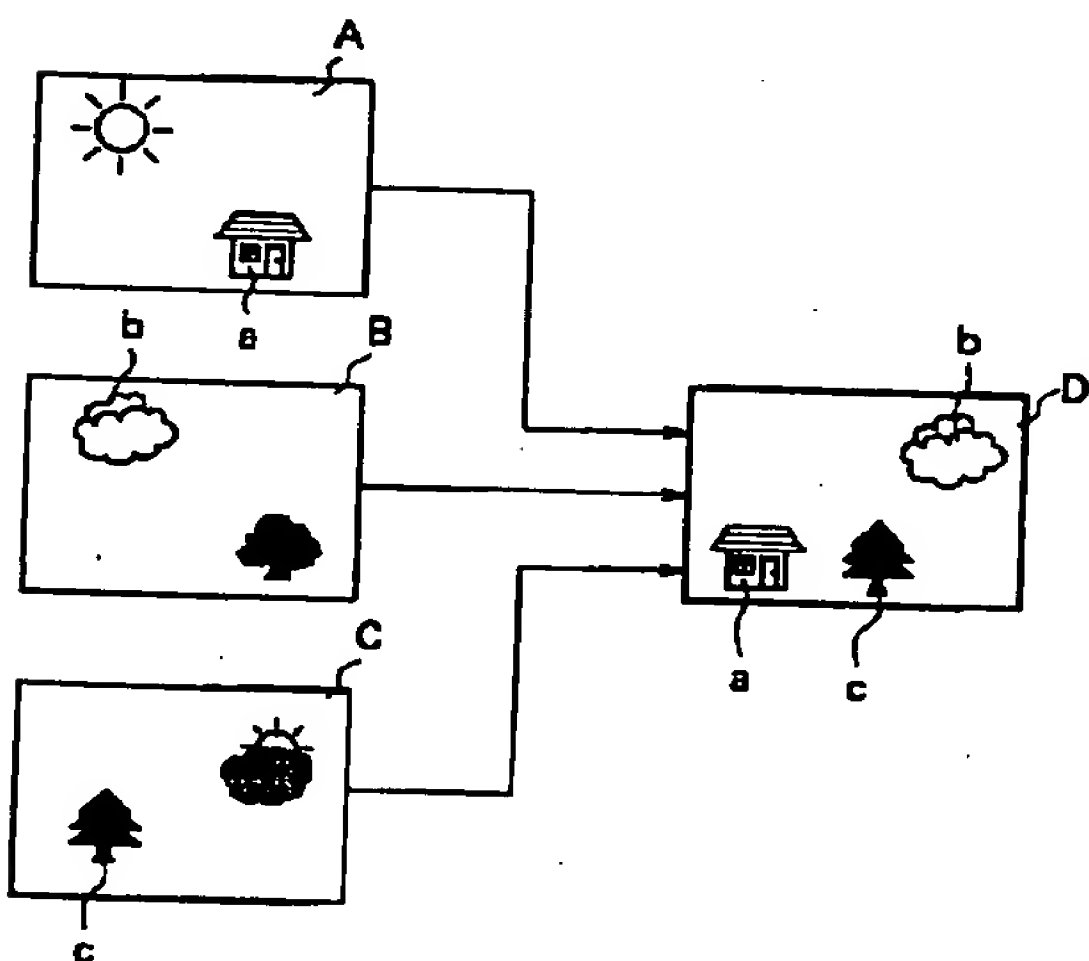
【図10】 本発明のデータ著作権管理システムで用い

るユーザ端末装置の実施例構成図。

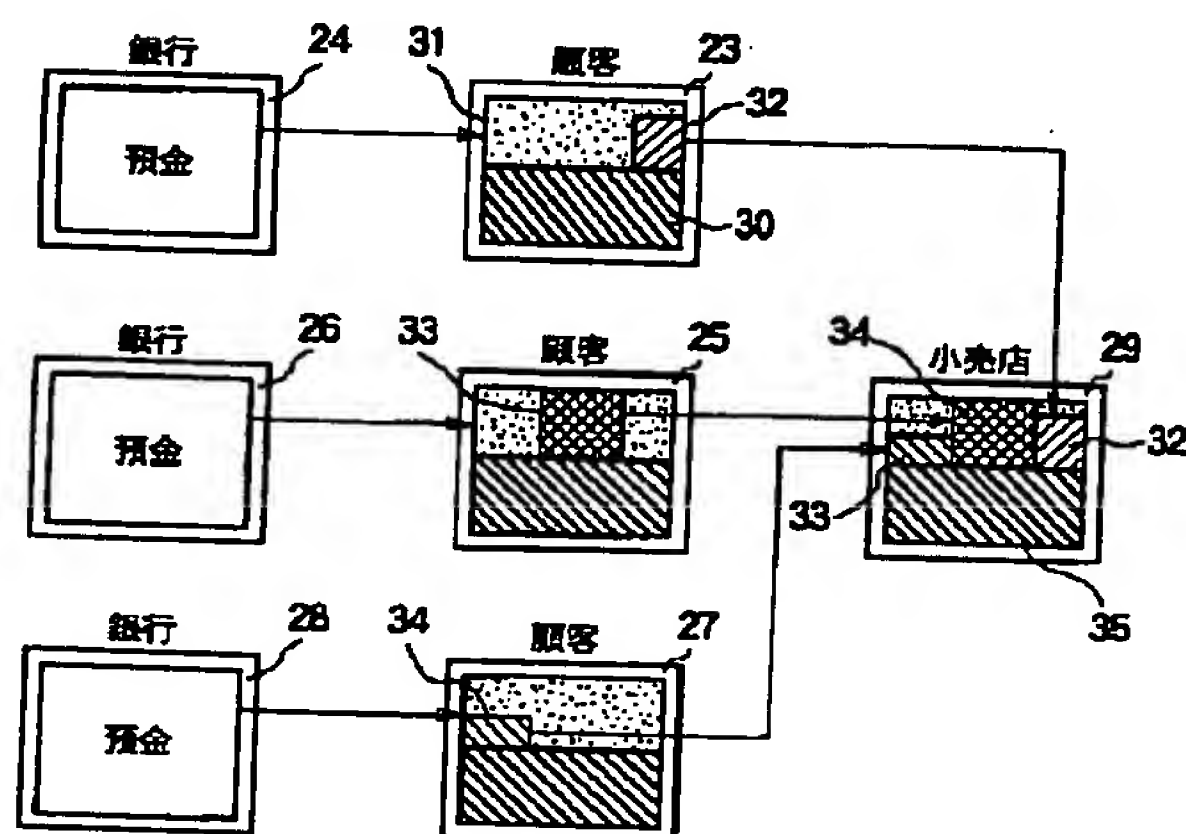
#### 【符号の説明】

- 1, 19, 20, 21 データベース
- 2 放送・通信衛星
- 3 11, 12, 13, 48, 49 記録媒体
- 4, 5, 6, 7 ユーザ端末装置
- 8 通信ネットワーク
- 9 鍵管理センタ
- 10, 14, 15, 17, 18 著作権管理センタ
- 23, 25, 27, 29 電子財布
- 24, 26, 28 預金口座
- 30, 35 残金
- 31 引出金
- 32, 33, 34 支払金
- 36 顧客
- 38 小売店
- 40 メーカ
- 37 顧客側銀行
- 39 小売店側銀行
- 41 メーカ側銀行
- 42, 43 ICカード
- 44, 45 テレビジョン会議参加者
- 46, 47 テレビジョン会議非参加者
- 50 マイクロプロセッサ
- 51 システムバス
- 52 PCカード
- 53 PCカードマイクロプロセッサ
- 54 PCカードマイクロプロセッサバス
- 55 読み出し専用メモリ
- 56 書き込み・読み出しメモリ

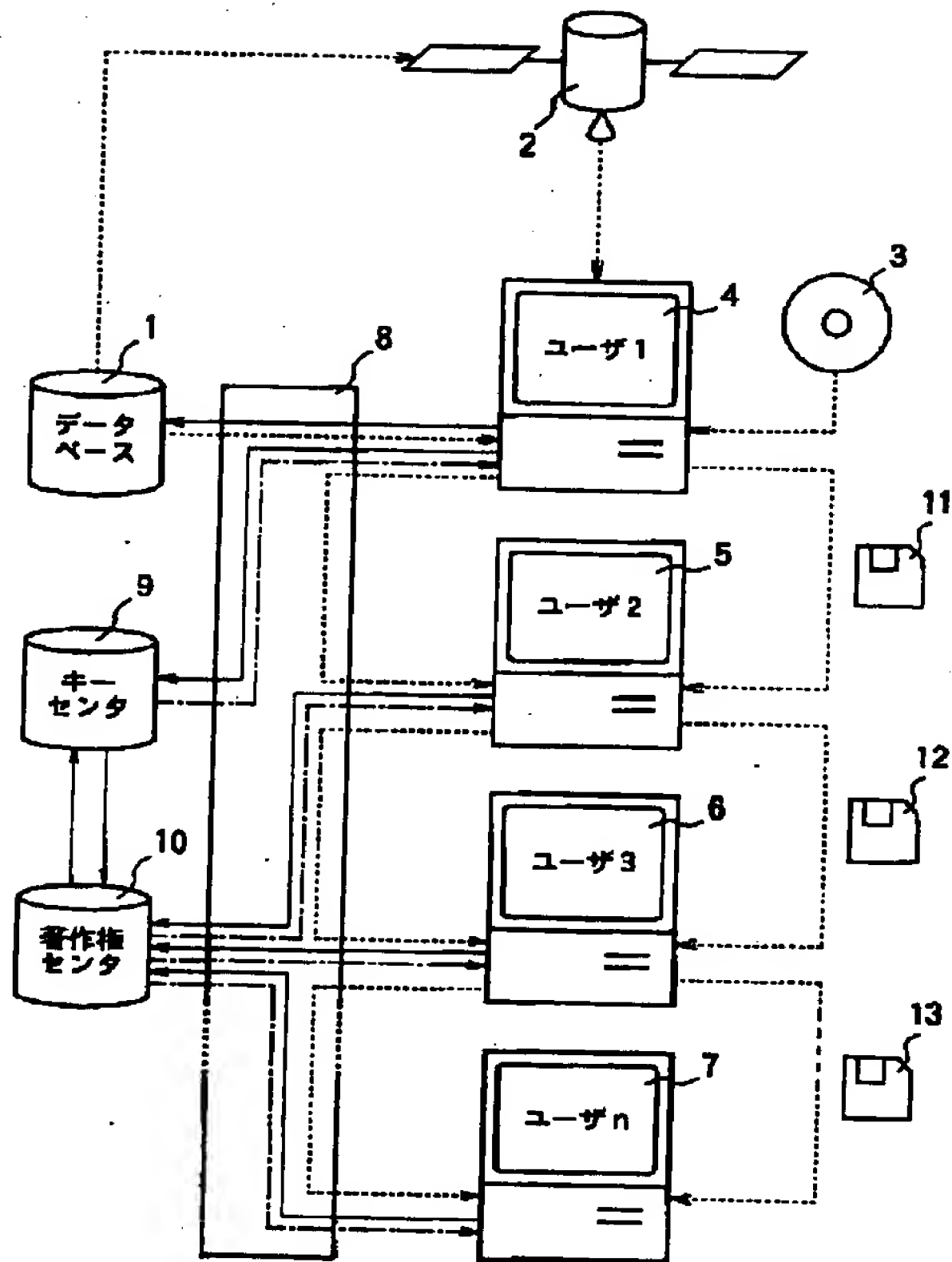
【図6】



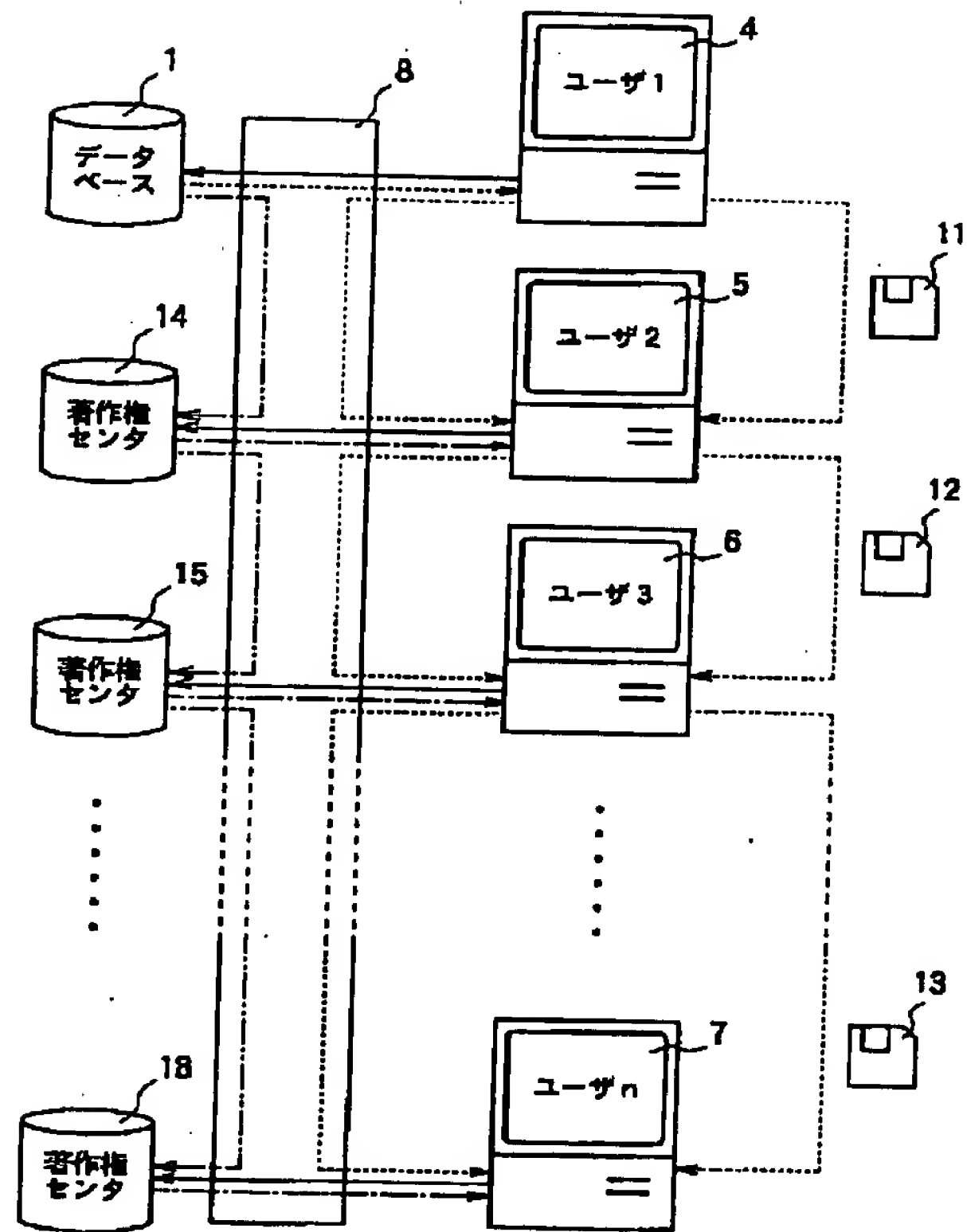
【図7】



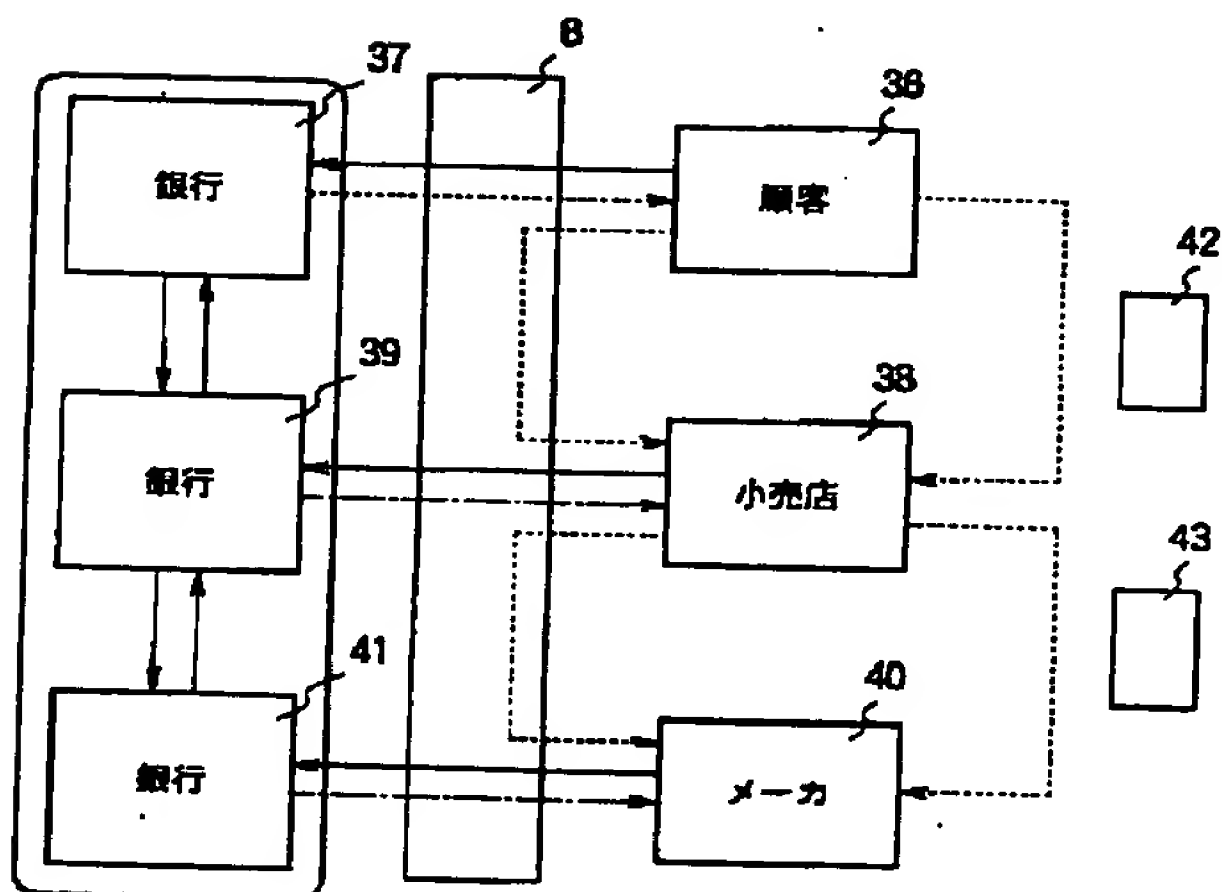
【図1】



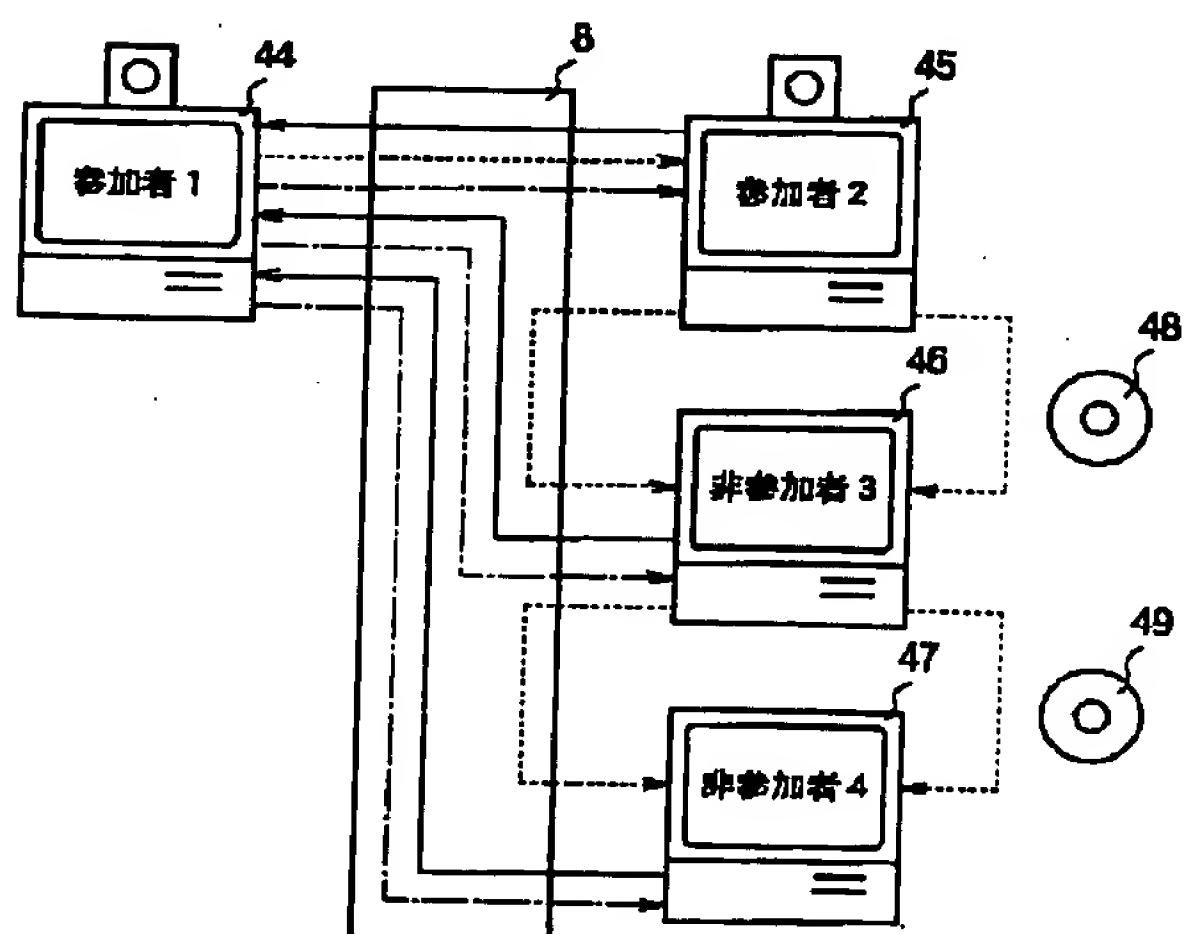
【図2】



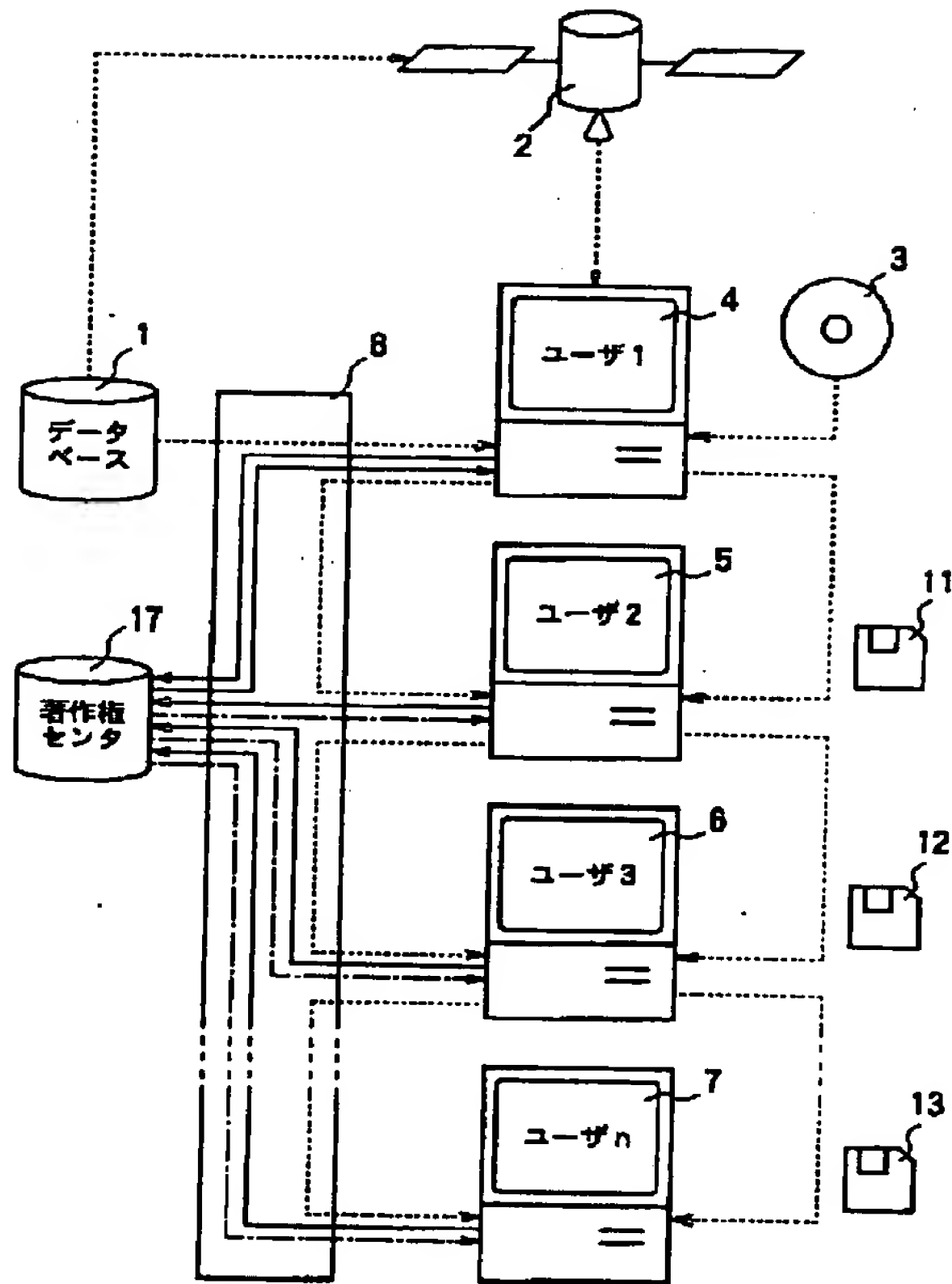
【図8】



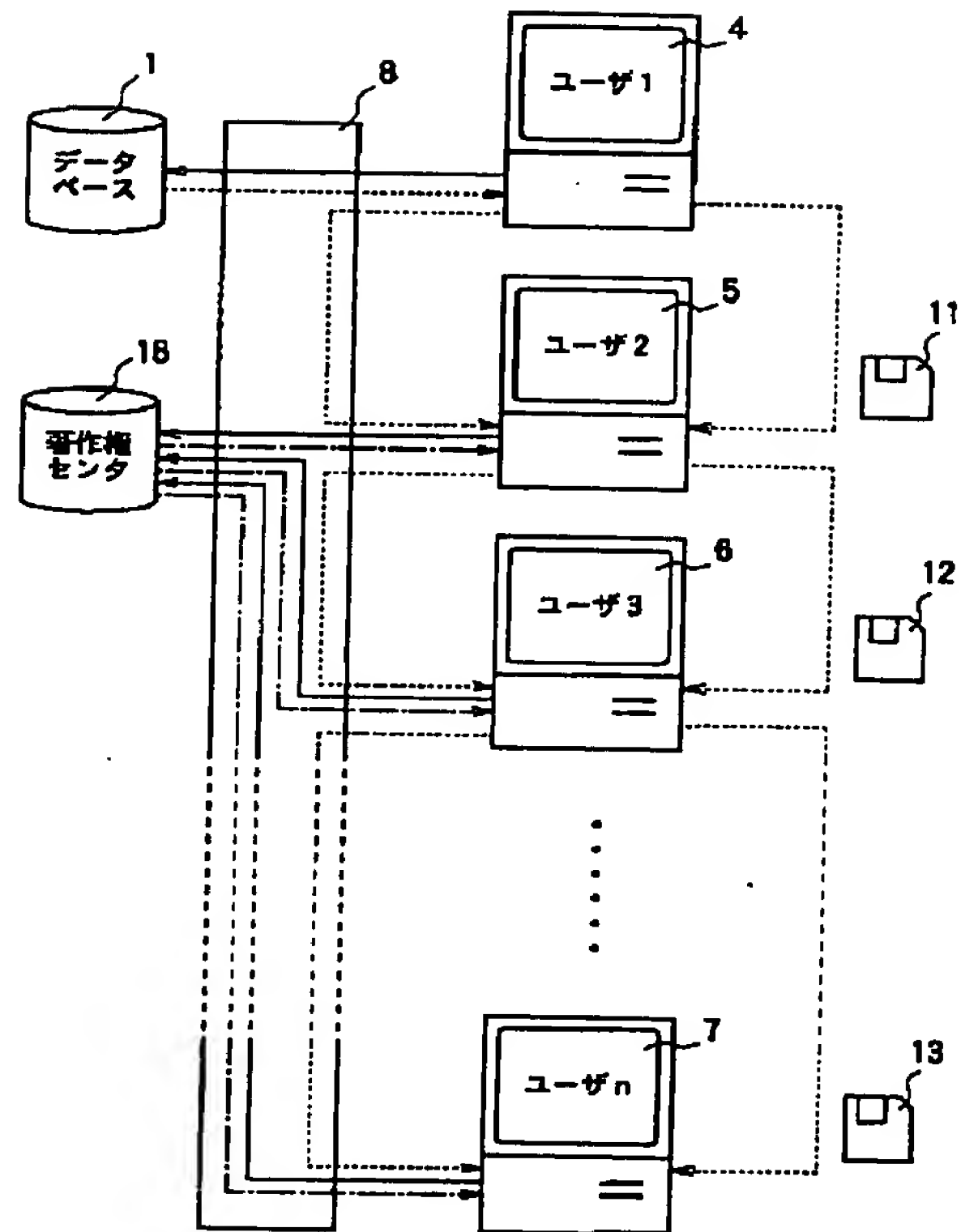
【図9】



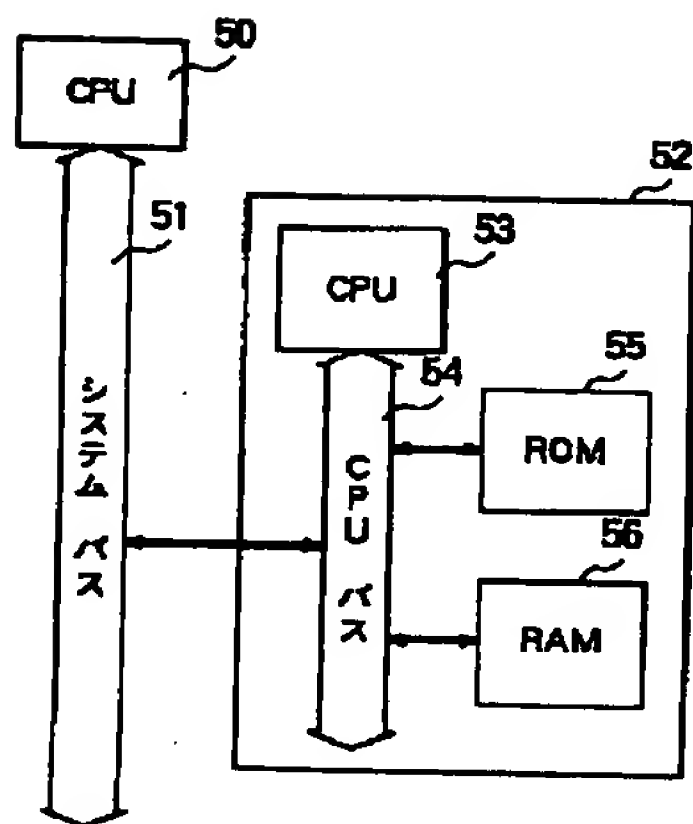
【図3】



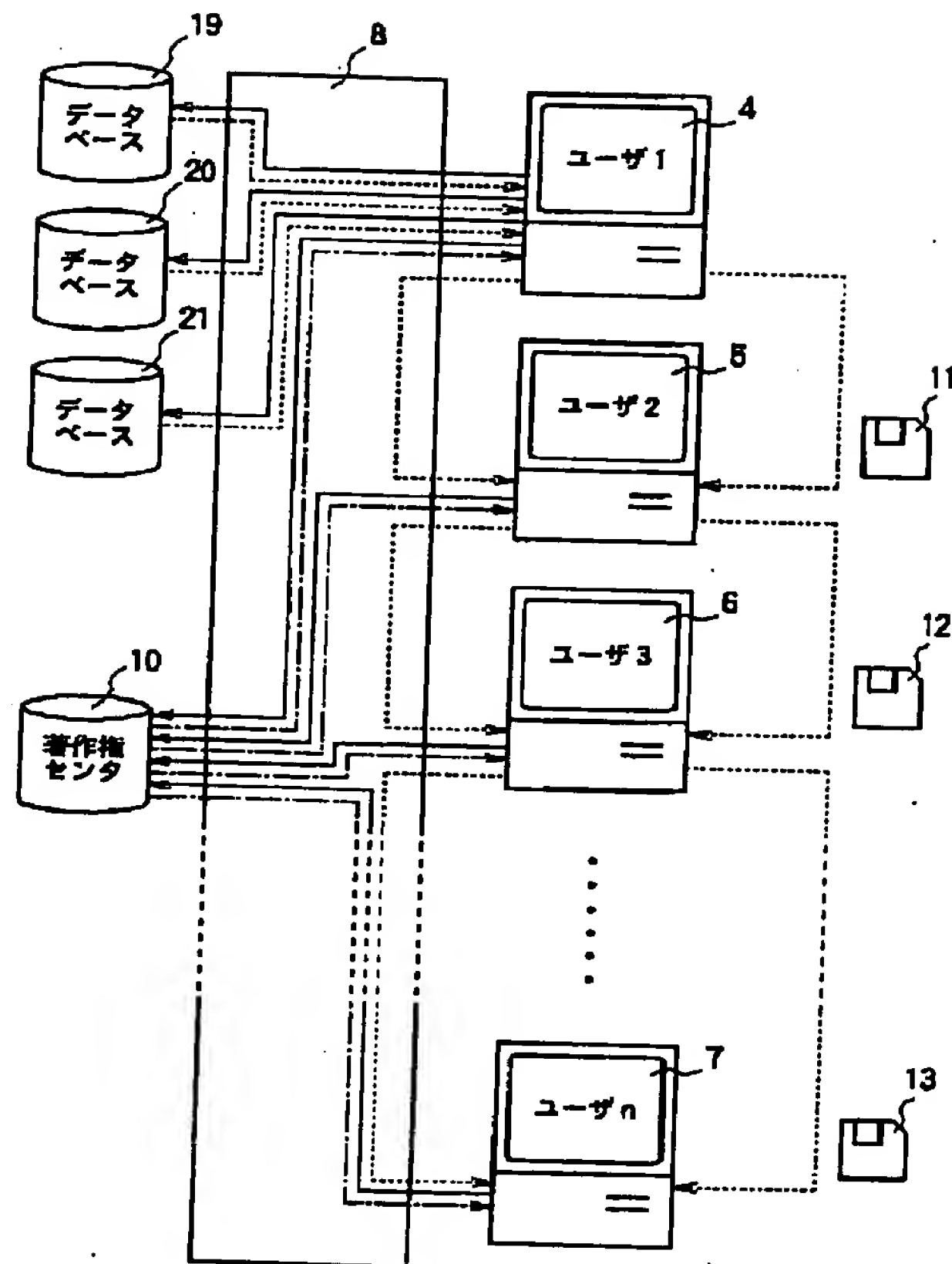
【図4】



【図10】



【図5】



フロントページの続き

(51)Int.Cl.<sup>6</sup>

H04L 9/00  
9/10  
9/12

識別記号

庁内整理番号

F I

技術表示箇所



(19)日本国特許庁 (JP)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号  
特開平8-292976

(43)公開日 平成8年(1996)11月5日

(51)IntCl.<sup>6</sup>  
G 0 6 F 17/60

識別記号 庁内整理番号

F I  
G 0 6 F 15/21

技術表示箇所  
Z

審査請求 未請求 請求項の数11 OL (全 7 頁)

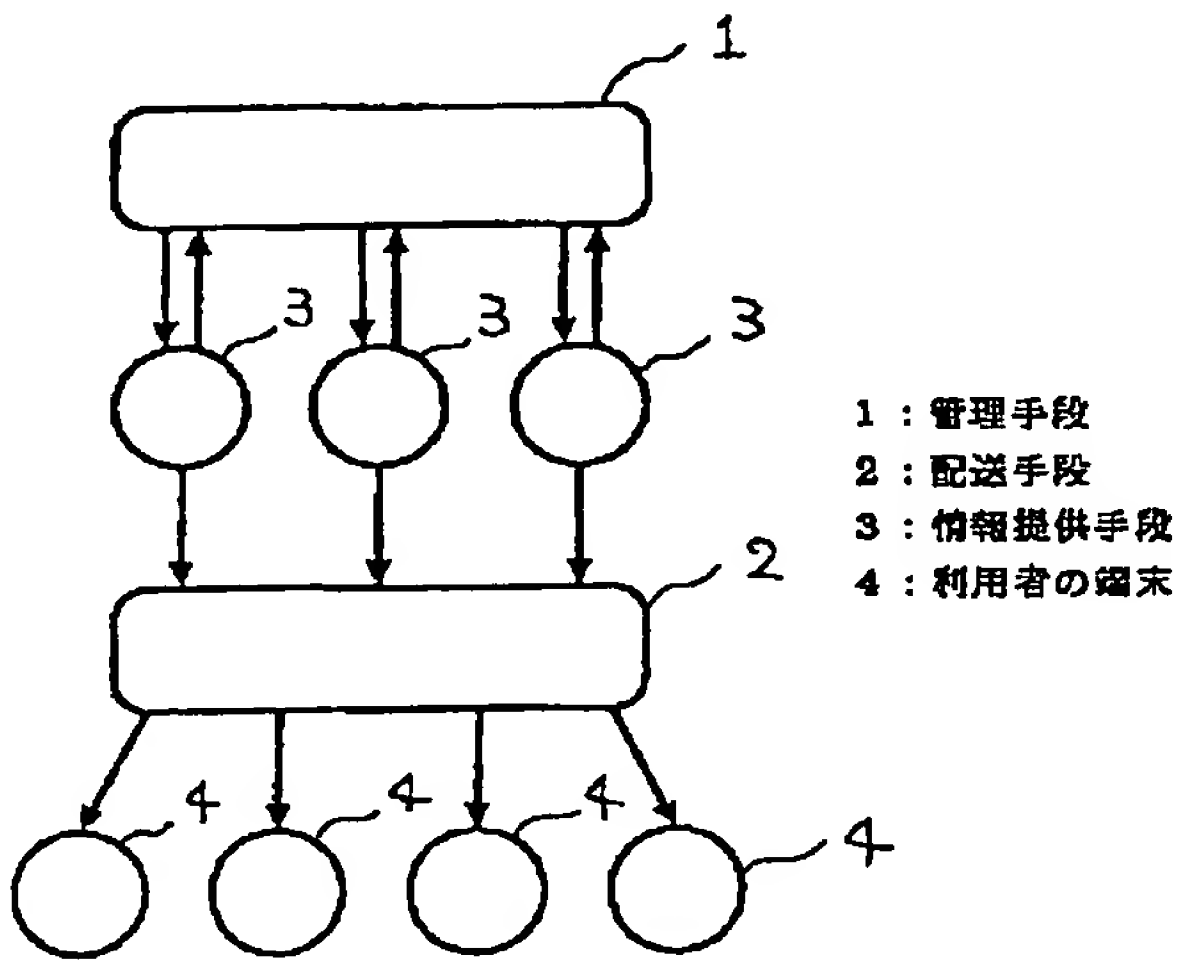
(21)出願番号	特願平7-96574	(71)出願人	000006013 三菱電機株式会社 東京都千代田区丸の内二丁目2番3号
(22)出願日	平成7年(1995)4月21日	(72)発明者	太田 英憲 鎌倉市大船五丁目1番1号 三菱電機株式 会社情報システム研究所内
		(72)発明者	山岸 篤弘 鎌倉市大船五丁目1番1号 三菱電機株式 会社情報システム研究所内
		(72)発明者	近澤 武 鎌倉市大船五丁目1番1号 三菱電機株式 会社情報システム研究所内
		(74)代理人	弁理士 宮田 金雄 (外3名)

(54) 【発明の名称】 著作権管理方式

(57) 【要約】

【目的】 著作物の不正な二次利用を検出し、不正利用しようという利用者に対して不正利用の抑止効果を持つ著作権管理方式を得ることを目的とする

【構成】 著作物を送付する情報提供手段3と、上記著作物が登録されるデータベースと、上記情報提供手段3により送付された著作物を受け取り、この著作物に二次利用の可否情報を記録して上記データベースに登録し、著作物に上記二次利用の可否情報が記録されているか否かをチェックする管理手段1と、利用者の端末4からの要求に基づいて上記データベースに登録した著作物を利用者の端末4に配送する配送手段2とを備えた。



## 【特許請求の範囲】

【請求項 1】 著作物を送付する情報提供手段と、上記著作物が登録されるデータベースと、上記情報提供手段により送付された著作物を受け取り、この著作物に二次利用の可否情報を記録して上記データベースに登録し、利用者からの要求に基づいて上記データベースに登録した著作物を利用者に配送し、著作物に上記二次利用の可否情報が記録されているか否かをチェックする管理配送手段とを備えたことを特徴とする著作権管理方式。

【請求項 2】 上記管理配送手段を、上記情報提供手段により送付された著作物を受け取り、この著作物に二次利用の可否情報を記録して上記データベースに登録し、著作物に上記二次利用の可否情報が記録されているか否かをチェックする管理手段と、利用者からの要求に基づいて上記データベースに登録された著作物を利用者に配送する配送手段とで構成したことを特徴とする請求項 1 記載の著作権管理方式。

【請求項 3】 上記管理手段は、上記管理手段のみがチェックできる二次利用の可否情報を記録することを特徴とする請求項 2 記載の著作権管理方式。

【請求項 4】 利用者により使用される端末を備え、上記管理手段は、利用者が上記端末によりチェックできる二次利用の可否情報を記録することを特徴とする請求項 2 記載の著作権管理方式。

【請求項 5】 上記管理手段は、上記管理手段の電子署名を上記著作物に行うことを特徴とする請求項 2 記載の著作権管理方式。

【請求項 6】 利用者により使用される端末を備え、上記配送手段は、利用者から要求された著作物の全体又は一部を上記端末に配送することを特徴とする請求項 2 記載の著作権管理方式。

【請求項 7】 上記端末は、上記配送手段により配送された著作物をこの著作物の種類に応じて出力する手段を備えたことを特徴とする請求項 6 記載の著作権管理方式。

【請求項 8】 上記配送手段は、利用者から要求された著作物を上記端末に暗号化して配送し、上記端末は、上記暗号化して配送された著作物を復号化する手段を備えたことを特徴とする請求項 6 記載の著作権管理方式。

【請求項 9】 利用者により使用され、上記配送手段に要求して上記著作物を受け取り、この著作物を用いて上記利用者により作成された新たな著作物を上記管理手段へ送付する端末を備え、上記管理手段は、上記利用者により作成された新たな著作物を受け取り、この新たな著作物が上記著作物の正当な二次利用か否かをチェックし、正当な二次利用のときに、上記新たな著作物に二次利用の可否情報を記録して上記データベースに登録することを特徴とする請求項 2 記載の著作権管理方式。

【請求項 10】 利用者により使用され、上記著作物の改変内容を上記管理手段へ通知し、さらに、上記管理手

段により改変された著作物を受け取り、この改変著作物を用いて上記利用者により作成された新たな著作物を上記管理手段へ送付する端末を備え、上記管理手段は、上記著作物の改変内容の通知を受け取り、上記著作物が二次利用可か否かをチェックし、二次利用可のときに、上記著作物を上記改変内容に基づいて改変し、この改変著作物を上記端末へ送付し、さらに、上記利用者により作成された新たな著作物を受け取り、この新たな著作物が上記著作物の正当な二次利用か否かをチェックし、正当な二次利用のときに、上記新たな著作物に二次利用の可否情報を記録して上記データベースに登録することを特徴とする請求項 2 記載の著作権管理方式。

【請求項 11】 利用者により使用され、上記著作物の改変内容と利用者自身の著作物とを上記管理手段へ送付する端末を備え、上記管理手段は、上記端末により送付されたものを受け取り、上記著作物が二次利用可か否かをチェックし、二次利用可のときに、上記著作物と上記著作物の改変内容と上記利用者自身の著作物とに基づいて新たな著作物を作成し、この新たな著作物に二次利用の可否情報を記録して上記データベースに登録することを特徴とする請求項 2 記載の著作権管理方式。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】 この発明は、利用者が著作物を二次利用する際の著作権保護に関するものである。

## 【0002】

【従来の技術】 近年、インターネットの発達、CD-ROMを使つてのソフトウェア流通、衛星を使ったデジタルデータの配送、VODの運用実験などが、注目を集めている。これらに共通した特徴は、マルチメディア化した情報、すなわち、大量データを持つ著作物を要求に応じて入手することができるシステムということである。例えば、インターネットでは、anonymous ftp, whois, wais, gopher, wwwなど各種ファイルサービスやデータベースサービスが提供されてきている。しかしながら、これらはほとんどがボランティアベースのサービスであり、提供される著作物も無償のものであった。

【0003】 有料の著作物を配布するためには、(1) 対価を払わなければ著作物を入手することができない、または著作物を入手したならば対価を必ず払わなければならない、(2) 著作物は改変されることなく、入手できないなければならない、(3) 入手した著作物を許可なくコピーして、第三者に配布することができない、といったようなことが守られなければならない。例えば、電子情報通信学会情報セキュリティ研究専門委員会が主催した“1995年暗号と情報セキュリティシンポジウムSCIS95”(1995年1月24日～27日)にて発表された「PCMCIAカードを利用した著作権保護システム」(NTTヒューマンインタフェース研究所、高嶋、石井、山中著)などのように、これまでは、(1)、(2)

については十分考えられているが、(3) に関してはあまり考慮されていなかった。そのため、有料の著作物はほとんど扱われることはなく、(1)、(2) の手段もほとんどとられていないのが現状である。

#### 【0004】

【発明が解決しようとする課題】従来の著作権管理方式は、一次利用に関して不正利用を防ぐことについて述べたものが多く、直接データベースから入手した著作物を加工する際に、不正な二次利用を防ぐ方法について述べられているものはない。

【0005】この発明は、ある一次著作物を加工して二次著作物を作成しても、一次著作物から引用したという事実が二次著作物に残り、不正に情報を第三者に流通させたとしても、情報の出所を容易に特定でき、不正利用の抑止効果を持つ著作権管理方式を得ることを目的とする。

#### 【0006】

【課題を解決するための手段】この第1の発明による著作権管理方式は、著作物を送付する情報提供手段と、上記著作物が登録されるデータベースと、上記情報提供手段により送付された著作物を受け取り、この著作物に二次利用の可否情報を記録して上記データベースに登録し、利用者からの要求に基づいて上記データベースに登録した著作物を利用者に配送し、著作物に上記二次利用の可否情報が記録されているか否かをチェックする管理配送手段とを備えたものである。

【0007】この第2の発明による著作権管理方式は、上記管理配送手段を、上記情報提供手段により送付された著作物を受け取り、この著作物に二次利用の可否情報を記録して上記データベースに登録し、著作物に上記二次利用の可否情報が記録されているか否かをチェックする管理手段と、利用者からの要求に基づいて上記データベースに登録された著作物を利用者に配送する配送手段とで構成したものである。

【0008】この第3の発明による著作権管理方式の管理手段は、管理手段のみがチェックできる二次利用の可否情報を記録するものである。

【0009】この第4の発明による著作権管理方式は、利用者により使用される端末を備え、上記管理手段は、利用者が上記端末によりチェックできる二次利用の可否情報を記録するものである。

【0010】この第5の発明による著作権管理方式の管理手段は、管理手段の電子署名を上記著作物に行うものである。

【0011】この第6の発明による著作権管理方式は、利用者により使用される端末を備え、上記配送手段は、利用者から要求された著作物の全体又は一部を上記端末に配送するものである。

【0012】この第7の発明による著作権管理方式の端末は、上記配送手段により配送された著作物をこの著作

物の種類に応じて出力する手段を備えたものである。

【0013】この第8の発明による著作権管理方式の配送手段は、利用者から要求された著作物を上記端末に暗号化して配送し、上記端末は、上記暗号化して配送された著作物を復号化する手段を備えたものである。

【0014】この第9の発明による著作権管理方式は、利用者により使用され、上記配送手段に要求して上記著作物を受け取り、この著作物を用いて上記利用者により作成された新たな著作物を上記管理手段へ送付する端末を備え、上記管理手段は、上記利用者により作成された新たな著作物を受け取り、この新たな著作物が上記著作物の正当な二次利用か否かをチェックし、正当な二次利用のときに、上記新たな著作物に二次利用の可否情報を記録して上記データベースに登録するものである。

【0015】この第10の発明による著作権管理方式は、利用者により使用され、上記著作物の改変内容を上記管理手段へ通知し、さらに、上記管理手段により改変された著作物を受け取り、この改変著作物を用いて上記利用者により作成された新たな著作物を上記管理手段へ送付する端末を備え、上記管理手段は、上記著作物の改変内容の通知を受け取り、上記著作物が二次利用可か否かをチェックし、二次利用可のときに、上記著作物を上記改変内容に基づいて改変し、この改変著作物を上記端末へ送付し、さらに、上記利用者により作成された新たな著作物を受け取り、この新たな著作物が上記著作物の正当な二次利用か否かをチェックし、正当な二次利用のときに、上記新たな著作物に二次利用の可否情報を記録して上記データベースに登録するものである。

【0016】この第11の発明による著作権管理方式は、利用者により使用され、上記著作物の改変内容と利用者自身の著作物とを上記管理手段へ送付する端末を備え、上記管理手段は、上記端末により送付されたものを受け取り、上記著作物が二次利用可か否かをチェックし、二次利用可のときに、上記著作物と上記著作物の改変内容と上記利用者自身の著作物とに基づいて新たな著作物を作成し、この新たな著作物に二次利用の可否情報を記録して上記データベースに登録するものである。

#### 【0017】

【作用】この第1の発明による著作権管理方式において、情報提供手段は著作物を送付し、管理配送手段は、上記情報提供手段により送付された著作物を受け取り、この著作物に二次利用の可否情報を記録して上記データベースに登録し、利用者からの要求に基づいて上記データベースに登録した著作物を利用者に配送し、著作物に上記二次利用の可否情報が記録されているか否かをチェックする。

【0018】この第2の発明による著作権管理方式において、管理手段は、上記情報提供手段により送付された著作物を受け取り、この著作物に二次利用の可否情報を記録して上記データベースに登録し、著作物に上記二次



利用の可否情報が記録されているか否かをチェックし、配送手段は、利用者からの要求に基づいて上記データベースに登録された著作物を利用者に配送する。

【0019】この第3の発明による著作権管理方式において、上記管理手段は、上記管理手段のみがチェックできる二次利用の可否情報を記録する。

【0020】この第4の発明による著作権管理方式において、上記管理手段は、利用者が端末によりチェックできる二次利用の可否情報を記録する。

【0021】この第5の発明による著作権管理方式において、上記管理手段は、上記管理手段の電子署名を上記著作物に行う。

【0022】この第6の発明による著作権管理方式において、上記配送手段は、利用者から要求された著作物の全体又は一部を利用者の端末に配送する。

【0023】この第7の発明による著作権管理方式において、上記端末は、上記配送手段により配送された著作物をこの著作物の種類に応じて出力する。

【0024】この第8の発明による著作権管理方式において、上記配送手段は、利用者から要求された著作物を上記端末に暗号化して配送し、上記端末は、上記暗号化して配送された著作物を復号化する。

【0025】この第9の発明による著作権管理方式において、利用者の端末は、上記配送手段に要求して上記著作物を受け取り、この著作物を用いて上記利用者により作成された新たな著作物を上記管理手段へ送付し、上記管理手段は、上記利用者により作成された新たな著作物を受け取り、この新たな著作物が上記著作物の正当な二次利用か否かをチェックし、正当な二次利用のときに、上記新たな著作物に二次利用の可否情報を記録して上記データベースに登録する。

【0026】この第10の発明による著作権管理方式において、利用者の端末は、上記著作物の改変内容を上記管理手段へ通知し、上記管理手段は、上記著作物の改変内容の通知を受け取り、上記著作物が二次利用可か否かをチェックし、二次利用可のときに、上記著作物を上記改変内容に基づいて改変し、この改変著作物を上記利用者の端末へ送付する。そして、上記端末は、上記管理手段により改変された著作物を受け取り、この改変著作物を用いて上記利用者により作成された新たな著作物を上記管理手段へ送付し、上記管理手段は、上記利用者により作成された新たな著作物を受け取り、この新たな著作物が上記著作物の正当な二次利用か否かをチェックし、正当な二次利用のときに、上記新たな著作物に二次利用の可否情報を記録して上記データベースに登録する。

【0027】この第11の発明による著作権管理方式において、利用者の端末は、上記著作物の改変内容と利用者自身の著作物とを上記管理手段へ送付し、上記管理手段は、上記端末により送付されたものを受け取り、上記著作物が二次利用可か否かをチェックし、二次利用可の

ときに、上記著作物と上記著作物の改変内容と上記利用者自身の著作物とに基づいて新たな著作物を作成し、この新たな著作物に二次利用の可否情報を記録して上記データベースに登録する。

【0028】

【実施例】

実施例1. 図1は、この発明の著作権管理方式の構成の一実施例を示す図である。以下、この発明の一実施例を図1を用いて説明する。図1において、1は著作権を管理する管理手段、2は著作物を配送する配送手段、3は著作物を提供する情報提供手段、4は著作物を利用する利用者の端末である。

【0029】まず、著作権を管理する管理手段1と著作物を配送する配送手段2を設ける。著作権を管理する管理手段1は、登録依頼があった著作物を登録するデータベースを有している。

【0030】情報提供手段3から著作物の登録依頼を受けた管理手段1は、テキスト、静止画、動画、音声等、その著作物の種類を考慮し、論理演算、ビット反転、シフト、回転、移動、複写等の1度ないし複数回の実施によって、著作権を管理する管理手段1に登録されている著作物であるということや、二次利用を許すか否か、または、著作物の登録番号等の、利用者には取り除くことのできない登録情報を、著作物の一部分、著作物の全体、著作物のある一定の単位、または、著作物の不定の単位毎に付加、または埋め込む。例えば、静止画像であれば矩形に区切られた単位、表示されているオブジェクト単位、また、動画画像であれば、フレーム単位、1フレームを静止画像と同様に区分した単位、フレームに含まれるオブジェクト単位等に埋め込むことが考えられる。この付加、あるいは埋め込まれた登録情報をチェックすることによって、著作権を管理する管理手段1に登録されている著作物であるということや、二次利用を許すか否か、または、著作物の登録番号等を知ることができる。

【0031】次に、管理手段1が、その登録情報が付加、あるいは埋め込まれた著作物全体に対し、配送の途中で著作物が改竄されても、利用者が改竄されたことを知ることができるように、管理手段1の電子署名を行い、著作物の登録番号等の登録情報と共に電子署名を行なった著作物を、管理手段1が有するデータベースに保存する。その後、管理手段1は、登録情報が付加、あるいは埋め込まれた著作物を情報提供手段3に戻す。

【0032】情報提供手段3は、登録情報が付加、あるいは埋め込まれた著作物を、配送手段2へ送信し、配送手段2は利用者の端末4から著作物を求められたときは、この登録情報が付加、あるいは埋め込まれた著作物を利用者に提供する。

【0033】実際に利用者の端末4に著作物を配送するためには、まず、利用者は端末4を用い配送手段2にユ



一ザ登録を行なって、ユーザIDをもらう。登録された利用者が端末4を用いて著作物の配送を要求すると、配送手段2は鍵を管理する機関（配送手段2自身、あるいは管理手段1、あるいは別に鍵を管理する第三の機関）に依頼して、ユーザID、著作物の登録番号に対応した配送用の暗号化鍵を入手する。配送手段2は入手した暗号化鍵を用いて著作物の暗号化を行ない、利用者の端末4に送信する。

【0034】利用者は入手した著作物を復号するために、端末4を用いて鍵を管理する機関に復号鍵の送信を依頼する。鍵を管理する機関は要求が正当なものと判断できれば、復号鍵を送信する。端末4は入手した復号鍵を使って暗号化された著作物を復号し、著作物の種類に対応した手段を用い、例えば、画像データならばディスプレイにイメージを表示する、音声データならばスピーカから音を出力するといった具合に、表示、または音声出力等の出力を行なう。

【0035】ある著作物が、管理手段1に登録されていることを利用者、または管理手段1が確かめるには、著作物の中に、管理手段1が関与したことを判別するための登録情報を付加、あるいは埋め込んでいるので、利用者の端末4、または管理手段1がその登録情報をチェックすることにより、実現できる。具体的には、画素を表示するために独自のパターンを使用するか、コピーライトの表示を入れたりすること等が考えられ、前者の場合には、管理手段1のみがチェックでき、後者の場合には、利用者の端末4がチェックできる。

【0036】次に、利用者が二次利用の許された著作物を加工したい場合を考える。利用者の端末4は二次利用を許す登録情報が付加、あるいは埋め込まれたその著作物を受け取り、著作物の全部、または一部を、付加、あるいは埋め込まれた登録情報ごと引用を行ない、加工する。そして、管理手段1へ加工後の二次著作物を送付して正当な二次利用かを確認してもらい、利用した一次著作物の部分に付加、あるいは埋め込まれた登録情報を取り除いて、二次著作物全体に新たな登録情報を付加、あるいは埋め込んでもらい、登録作業をしてもらう。登録せずに流通させると、不正に加工を行ったことになる。この不正加工は管理手段1が認識可能である。原著作物に二次使用許諾が無い場合や、加工後の二次著作物を送付しない場合などには、不正な二次使用となり、利用者は作成した二次著作物を登録できない。

【0037】こうしてある登録情報が付加、あるいは埋め込まれた二次著作物は配送手段2へ送られる。引用された一次著作物の利用条件（加工物を流通させても良い等）に従う限りは、一般の一次著作物と同じように流通させることができる。

【0038】実施例2. なお、上記実施例1では、著作権を管理する管理手段1と著作物を配送する配送手段2は、それぞれ一つずつ設けたが、一体となっても構わな

い（図2）。図2に示した構成の場合、配送手段2は、管理手段1が有するデータベースを直接アクセスし、利用者が要求した著作物を利用者の端末4に配送しても良い。また、著作権を管理する管理手段1と著作物を配送する配送手段2をそれぞれ複数設けても構わない（図3）。図3に示した構成の場合、登録情報が付加、あるいは埋め込まれた著作物を管理手段1が配送手段2に送付し、配送手段2は、複数の管理手段1から送付された著作物を配送手段2が有するデータベースに保存するようにしても良い。

【0039】実施例3. この実施例3では、利用者が二次利用の許された著作物を加工したい別な場合を考える。まず利用者は、端末4を用いて著作物を配送してもらう。次に利用者は、端末4を用いてその著作物をどのように改変したいかを管理手段1へ通知し、管理手段1が二次使用許諾のある著作物であるという確認後、指定された改変を行い、登録情報を付加、あるいは埋め込んで、結果を利用者の端末4に戻す。そこで得られた結果を利用者自身の著作物中で使用し、管理手段1で登録作業をしてもらう。

【0040】実施例4. 上記実施例3では、管理手段1が改変後、利用者の端末4に結果を戻して利用者の端末4側で自身の著作物の中に入れて新著作物を作成しているが、この作業をすべて管理手段1にやらせてもよい。この場合、利用者の端末4はその著作物をどのように改変したいかを、利用者自身の著作物の中でどのように使用したいかの指示、および利用者自身の著作物と共に管理手段1へ通知し、管理手段1が二次使用許諾のある著作物であるという確認後、指定された改変を行い、さらに、利用者の指示による新著作物を作成する。ここで、登録情報を付加、あるいは埋め込んで、登録作業を行う。

【0041】実施例5. 利用者がある著作物を、加工せずにそのまま利用したい場合も、上記実施例1と同様に、二次使用許諾を受け取ってから利用させるようにする。これにより、不正コピー等が防止できる。

【0042】実施例6. 著作物を配送する配送手段2は、利用者の端末4から著作物の配送を要求された場合、要求された著作物の全体、または一部を送付することにする。具体的には、ある登録情報が付加、あるいは埋め込まれた著作物の全データを送る方法や、表示や出力を行うのみのデータを送る方法等が考えられる。

【0043】実施例7. 著作権を管理する管理手段1は、登録情報を著作物に付加、あるいは埋め込むが、通常的手段で出力したのでは著作物の品質が劣化したまま出力されるような登録情報を付加、あるいは埋め込むようにすることもできる。この場合には、不正利用される著作物は品質が劣化しているため、不正に流通することに対する問題も少なくなる。

【0044】

【発明の効果】以上のように、この第1の発明によれば、著作物を送付する情報提供手段と、上記著作物が登録されるデータベースと、上記情報提供手段により送付された著作物を受け取り、この著作物に二次利用の可否情報を記録して上記データベースに登録し、利用者からの要求に基づいて上記データベースに登録した著作物を利用者に配送し、著作物に上記二次利用の可否情報が記録されているか否かをチェックする管理配送手段とを備えたことにより、著作物の不正な二次利用を検出できるので、不正利用しようという利用者に対する抑止効果を得ることができる。

【0045】この第2の発明によれば、上記管理配送手段を、上記情報提供手段により送付された著作物を受け取り、この著作物に二次利用の可否情報を記録して上記データベースに登録し、著作物に上記二次利用の可否情報が記録されているか否かをチェックする管理手段と、利用者からの要求に基づいて上記データベースに登録された著作物を利用者に配送する配送手段とで構成したことにより、管理手段と配送手段とで著作権管理の負荷が分散するので、効率良く著作権が管理できる。

【0046】この第3の発明によれば、上記管理手段は、上記管理手段のみがチェックできる二次利用の可否情報を記録するので、上記二次利用の可否情報を不正に書き換えることができないという効果がある。

【0047】この第4の発明によれば、上記管理手段は、利用者が端末によりチェックできる二次利用の可否情報を記録するので、利用者も不正な二次利用を検出でき、不正利用しようという利用者に対する抑止効果を得ることができる。

【0048】この第5の発明によれば、上記管理手段は、上記管理手段の電子署名を上記著作物に行うので、配送の途中で著作物が改竄されても、利用者が改竄されたことを知ることができる。

【0049】この第6の発明によれば、上記配送手段は、利用者から要求された著作物の全体又は一部を利用者の端末に配送するので、全体を必要とする利用者と一部を必要とする利用者のどちらの要求にも応じることができる。

【0050】この第7の発明によれば、上記端末は、上記配送手段により配送された著作物をこの著作物の種類に応じて出力する手段を備えたので、多種類の著作物を出力できる。

【0051】この第8の発明によれば、上記配送手段は、利用者から要求された著作物を上記端末に暗号化して配送し、上記端末は、上記暗号化して配送された著作物を復号化する手段を備えたので、不当な利用者は上記著作物を利用できないという効果がある。

【0052】この第9の発明によれば、利用者により使用され、上記配送手段に要求して上記著作物を受け取り、この著作物を用いて上記利用者により作成された新

たな著作物を上記管理手段へ送付する端末を備え、上記管理手段は、上記利用者により作成された新たな著作物を受け取り、この新たな著作物が上記著作物の正当な二次利用か否かをチェックし、正当な二次利用のときに、上記新たな著作物に二次利用の可否情報を記録して上記データベースに登録することにより、一部を加工して新たに作成した著作物を不正に流通させようとしても、一次著作物の不正使用が、加工後の著作物から読みとることができるので、不正利用しようという利用者に対する抑止効果を得ることができる。

【0053】この第10の発明によれば、利用者により使用され、上記著作物の改変内容を上記管理手段へ通知し、さらに、上記管理手段により改変された著作物を受け取り、この改変著作物を用いて上記利用者により作成された新たな著作物を上記管理手段へ送付する端末を備え、上記管理手段は、上記著作物の改変内容の通知を受け取り、上記著作物が二次利用可か否かをチェックし、二次利用可のときに、上記著作物を上記改変内容に基づいて改変し、この改変著作物を上記端末へ送付し、さらに、上記利用者により作成された新たな著作物を受け取り、この新たな著作物が上記著作物の正当な二次利用か否かをチェックし、正当な二次利用のときに、上記新たな著作物に二次利用の可否情報を記録して上記データベースに登録することにより、一部を加工して新たに作成した著作物を不正に流通させようとしても、一次著作物の不正使用が、加工後の著作物から読みとることができるので、不正利用しようという利用者に対する抑止効果を得ることができる。

【0054】この第11の発明によれば、利用者により使用され、上記著作物の改変内容と利用者自身の著作物とを上記管理手段へ送付する端末を備え、上記管理手段は、上記端末により送付されたものを受け取り、上記著作物が二次利用可か否かをチェックし、二次利用可のときに、上記著作物と上記著作物の改変内容と上記利用者自身の著作物とに基づいて新たな著作物を作成し、この新たな著作物に二次利用の可否情報を記録して上記データベースに登録することにより、一部を加工して新たに作成した著作物を不正に流通させようとしても、一次著作物の不正使用が、加工後の著作物から読みとることができるので、不正利用しようという利用者に対する抑止効果を得ることができる。

#### 【図面の簡単な説明】

【図1】 この発明の実施例1の著作権管理方式の構成図である。

【図2】 この発明の著作権管理方式の他の構成図である。

【図3】 この発明の著作権管理方式のさらに他の構成図である。

#### 【符号の説明】

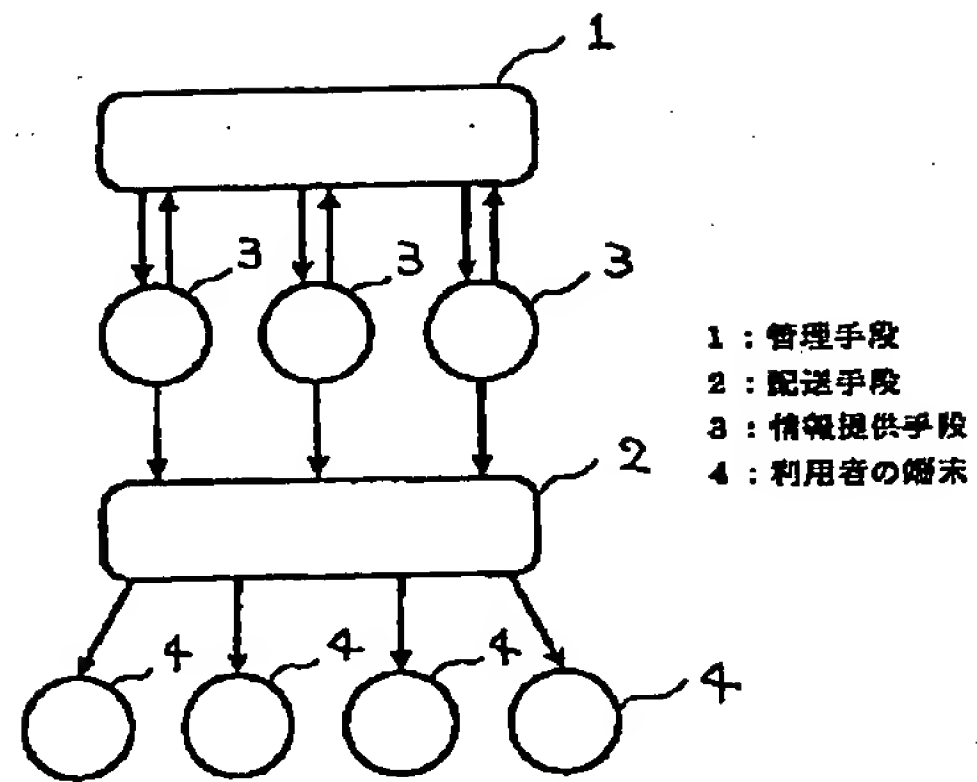
1 管理手段、2 配送手段、3 情報提供手段、4

(7)

11

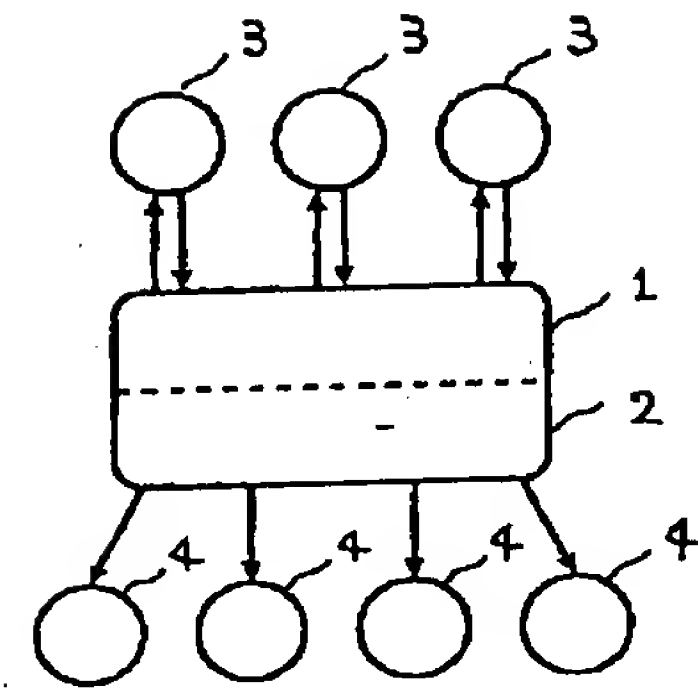
利用者の端末

【図1】

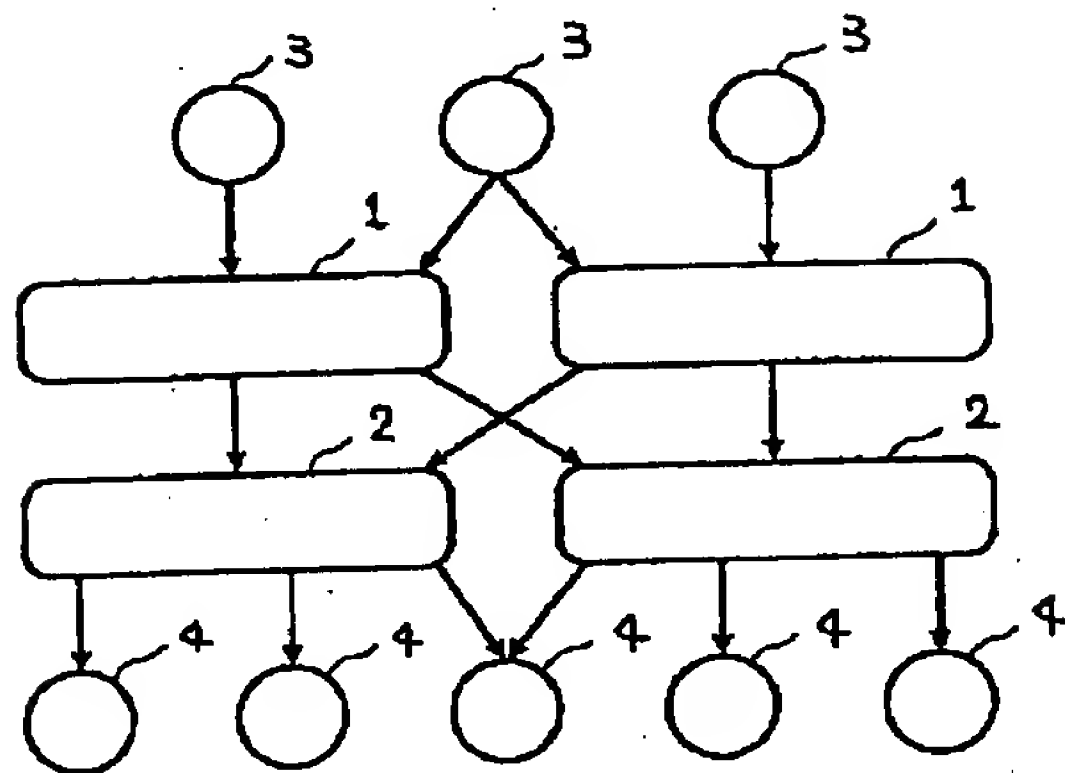


12

【図2】



【図3】



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-329011

(43) 公開日 平成8年(1996)12月13日

(51) Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0	9364-5L	G 0 6 F 15/00	3 3 0 Z
12/00	5 3 7	7623-5B	12/00	5 3 7 H
17/60		7259-5J	G 0 9 C 1/00	
G 0 9 C 1/00			G 0 6 F 15/21	Z
H 0 4 L 9/06			H 0 4 L 9/02	Z

審査請求 未請求 請求項の数 2 O L (全 10 頁) 最終頁に続く

(21) 出願番号 特願平7-136808

(22) 出願日 平成7年(1995)6月2日

(71) 出願人 000005979

三菱商事株式会社

東京都千代田区丸の内2丁目6番3号

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 斎藤 誠

東京都千代田区丸の内二丁目6番3号 三

菱商事株式会社内

(72) 発明者 岡崎 正一

神奈川県鎌倉市上町屋325番地 三菱電機

株式会社情報システム製作所内

(74) 代理人 弁理士 南條 眞一郎

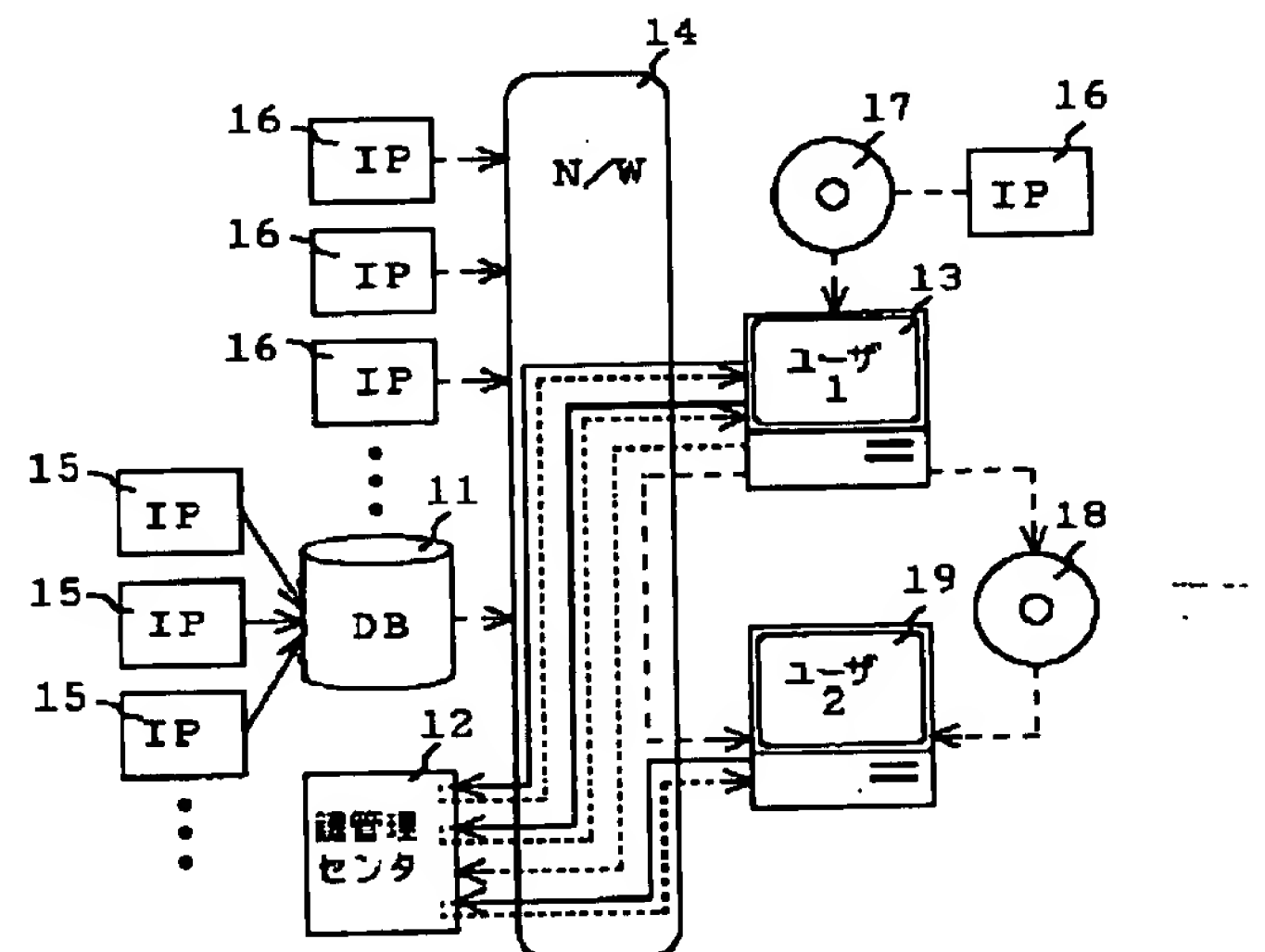
(54) 【発明の名称】 データ著作権管理システム

(57) 【要約】

【目的】 1次ユーザが入手したデータを加工し、加工されたデータを2次利用者へ供給するデータ著作権管理システムを提供する。

【構成】 データベース、鍵管理センタを備え、1次著作権ラベル、第1暗号鍵を含む1次利用鍵、2次利用鍵、第3暗号鍵、著作権管理プログラムが用いられる。

1次ユーザは第1暗号鍵を用いて暗号化されて供給された1次著作権データを鍵管理センタから入手した1次利用鍵で平文化し利用するが、保存する場合には1次利用鍵を用いて再暗号化される。1次ユーザは鍵管理センタから1次著作権データ加工用の2次利用鍵を入手して1次著作権データの加工を行い、加工途中のデータは2次利用鍵で暗号化されて保存される。1次ユーザは加工が終了すると2次著作権兼用の第3暗号鍵を鍵管理センタから受け取り、加工済みデータを第3暗号鍵で暗号化し、2次ユーザに配布する。2次ユーザは鍵管理センタから第3暗号鍵を入手し、加工データを利用する。





## 【特許請求の範囲】

【請求項1】 データベースおよび鍵管理センタを備え、データ著作物を入手した1次ユーザが入手した1次著作権データを加工し、加工によって得られた2次著作権データを2次利用者へ供給する場合に著作権を管理するデータ著作権管理システムであって：前記1次著作権データが1次利用鍵を用いて暗号化されて前記1次ユーザに供給され；前記1次著作権データの利用を希望する前記1次ユーザからの前記1次利用鍵の配布要求に対し、前記鍵管理センタが前記1次利用鍵を前記1次ユーザに配布し；前記1次ユーザは配布された前記1次利用鍵を用いて前記1次著作権データを平文化して1次利用を行い；前記1次著作権データの加工を希望する前記1次ユーザは前記鍵管理センタから前記1次著作権データを加工するための2次利用鍵の配布を受け、配布された前記第2利用鍵を用いて前記1次著作権データの加工を行い、加工中の著作権データは前記第2利用鍵を用いて暗号化されて保存され；加工が終了した前記1次ユーザは前記鍵管理センタから加工済みデータを配布するための第3暗号鍵の配布を受け、前記加工済みデータを前記第3暗号鍵を用いて暗号化して2次ユーザに供給し；前記2次著作権データの利用を希望する前記2次ユーザは前記鍵管理センタから前記第3暗号鍵の配布を受け、配布された前記第3暗号鍵を用いて前記2次著作権データを平文化して利用する；データ著作権管理システム。

【請求項2】 前記1次ユーザによる前記1次著作権データの加工が、前記1次著作権データの複写物に対して行われる請求項1記載のデータ著作権管理システム。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】 本発明はデジタルデータの利用、すなわち表示、保存、複写、加工、転送において著作権を管理するシステムに係るものである。

## 【0002】

【従来の技術】 情報化時代と言われる今日、通常の上波放送(terrestrial broadcasting)の他に放送衛星(Broadcasting Satellite: BS)、通信衛星(Communication Satellite: CS)と呼ばれる衛星放送、同軸ケーブルあるいは光ケーブルを利用したCATV(Cable Television)と呼ばれる有線TV放送が普及しつつある。

【0003】 同時に数10チャンネルを配信することができる衛星放送あるいはCATV放送においては、包括的な契約によって視聴することができるスクランブルがかけられていない一般的なチャンネルの他に、包括的な契約によっては視聴することができないスクランブルされた映画・スポーツ・音楽等専門的なチャンネルが設けられている。これらのチャンネルを視聴するためにはスクランブルを解除するするために契約を行う必要があるが、この契約期間は通常1カ月程度の単位で行われるため、随時の契約によって視聴することができない。

【0004】 この問題に対応するために、本発明者らは特開平6-46419号及び特開平6-141004号で公衆電信電話回線を通じて課金センタから視聴許可鍵を入手するとともに課金が行われ、視聴許可鍵を用いて番組毎に異なるスクランブルパターンで行われたスクランブルを解除して番組を視聴するシステムを、特開平6-132916号でそのための装置を提案した。これらのシステム及び装置において、スクランブルされた番組の視聴を希望する者は通信装置を使用し通信回線を経由して課金センタに視聴申し込みを行い、課金センタはこの視聴申し込みに対して通信装置に許可鍵を送信するとともに課金処理を行い料金を徴収する。通信装置で許可鍵を受信した視聴希望者は通信装置と受信装置を接続する直接的な手段あるいはフレキシブルディスク等の間接的な手段によって許可鍵を受信装置に送り込み、許可鍵を送り込まれた受信装置はその許可鍵によって番組のスクランブルを解除する。

【0005】 特開平6-132916号にはこれらのシステム及び装置の応用として、各々異なるスクランブルパターンでスクランブルされた複数のデータが記録されたテープあるいはディスクを販売あるいは貸与し、ICカード等により許可鍵を供給して特定のデータを利用するシステム及び装置も記載されている。

【0006】 また、情報化時代と呼ばれる今日、これまでは各々のコンピュータが独立して保存していた各種のデータをLAN(Local Area Network)と呼ばれる局所的ネットワーク、WAN(Wide Area Network)と呼ばれる国単位のネットワークさらにはこれらを国際的に拡大したインターネット(Internet)と呼ばれるネットワークによってコンピュータ通信ネットワークシステムを構成し、相互に利用するデータベースシステムが普及しつつある。

【0007】 一方、デジタル化すると情報量が膨大になるためデジタル化することができなかったテレビジョン動画信号を圧縮することにより情報量を減少させ、実用的なデジタル化を可能にする技術が開発され、これまでにテレビジョン会議用のH.261規格、静止画像用のJPEG(Joint Photographic image coding Experts Group)規格、画像蓄積用のMPEG1(Moving Picture image coding Experts Group 1)規格及び現在のテレビジョン放送から高精細度テレビジョン放送に対応するMPEG2規格が作成された。

【0008】 これらの画像圧縮技術を利用したデジタル化技術はテレビジョン放送あるいはビデオ画像記録用に用いられるだけではなく、コンピュータでこれまで扱うことができなかったテレビジョン動画データが扱うことができるようになり、コンピュータが扱う各種のデータとデジタル化されたテレビジョン動画データを同時に取り扱う「マルチメディアシステム」が将来の技術として注目されている。このマルチメディアシステムもデータ

通信に組み入れられ、データベース上のデータの一つとして利用される。

【0009】このようにしてデータベースの利用範囲が拡大する中で、データベース上のデータ利用に対する課金をどのようにして行うかということ及びデータの直接的な利用以外の複写あるいは転送等によって発生する著作権の問題及びデータの加工によって発生する2次的著作権の問題をどのようにして処理するかということが重要になる。課金及び著作権の処理を確実に行うには、正規の利用者でなければデータの利用が不可能であるようにする必要があり、データを暗号化しておくことがそのための最良の手段である。

【0010】これらのテレビジョンシステムあるいはデータベースシステムにおいて、データを暗号化し、暗号化されたデータを復号して利用するためには暗号鍵が必要であり、データ利用者に対して暗号鍵を渡さなければならないが、この作業は安全性及び確実性が要求されるため非常に煩雑である。

【0011】本発明はその構成において暗号技術が重要な役割を果たすが、初めに一般的な暗号技術について説明する。暗号技術においては、平文Mを暗号鍵Kを用いて暗号化し暗号文Cを得る暗号化(Encryption)を  $C = E(K, M)$  と表現し、暗号文Cを暗号鍵Kを用いて復号化し平文Mを得る復号化(Decryption)を  $M = D(K, C)$  と表現する。

【0012】さらに、本発明者らは特願平6-64889号においてデータ著作権管理システムの具体的な構成を提案した。このシステムでは、デジタル映像のリアルタイム送信も含むデータベースシステムにおけるデジタルデータの表示(音声化を含む)、保存、複写、加工、転送における著作権の管理を行うために、利用申し込み者に対して暗号化されたデータの利用を許可する鍵の他に、必要に応じて著作権を管理するためのプログラム、著作権情報あるいは著作権管理メッセージの何れか一つあるいは複数を送信する。著作権管理メッセージは申し込みあるいは許可内容に反する利用が行われようとした場合に画面に表示され、ユーザに対して注意あるいは警告を行い、著作権管理プログラムは申し込みあるいは許可内容に反する利用が行われないように監視し管理を行う。

【0013】また、データは暗号化されて供給され、許可鍵を用いて復号化され利用されるが、装置内への保存、装置外の媒体への複写、装置外への転送が行われる場合には暗号化される。また、表示・利用、保存、複写、加工、転送等の利用形態各々に対して許可鍵が用意される。

【0014】

【発明の概要】本発明のシステムはデータベース、鍵管

理センタ、1次ユーザ、2次ユーザおよびこれらを相互に接続するネットワークシステムから構成され、1次著作権ラベル、第1暗号鍵を含む1次利用鍵、第2暗号鍵を含む2次利用鍵、2次著作権ラベル、第3暗号鍵、著作権管理プログラムが用いられる。平文1次著作権データは1次暗号鍵を用いて暗号化された状態で、1次ユーザに供給され、暗号1次著作権データの利用を希望する1次ユーザは、鍵管理センタにネットワークシステムを経由して1次利用鍵の配布を要求し、1次ユーザからの1次利用鍵の配布要求を受けた鍵管理センタは1次利用鍵を1次ユーザに配布し、このときに課金を行う。

【0015】1次ユーザは配布された1次利用鍵に含まれる第1暗号鍵を用いて暗号化1次著作権データを平文化し利用するが、平文1次著作権データを1次ユーザの装置内へ保存する場合には1次利用鍵を用いて再暗号化される。1次著作権データの加工を希望する1次ユーザが平文1次著作権データの加工を行うための2次利用鍵の配布をネットワークシステムを経由して鍵管理センタに要求すると、鍵管理センタは2次利用鍵を1次ユーザに配布する。2次利用鍵を受け取った1次ユーザは1次著作権データの複写を作成し、複製された1次著作権データの加工を行い、加工途中の平文2次著作権データを2次利用鍵に含まれた第2暗号鍵により暗号化し、最終加工データは第3暗号鍵を用いて暗号化して1次ユーザの装置内に保存する。1次ユーザは2次著作権データのデータ加工についての2次著作権を行使するために鍵管理センタに第3暗号鍵を登録し、暗号2次著作権データを第3暗号鍵を用いて暗号化して外部記憶媒体への複写あるいはネットワークシステムを介して転送することにより2次ユーザへ供給する。

【0016】暗号2次著作権データの利用を希望する2次ユーザは、鍵管理センタに第3暗号鍵の配布を要求し、第3暗号鍵の配布要求を受けた鍵管理センタは、第3暗号鍵をネットワークシステムを経由して2次ユーザに配布する。2次暗号鍵を受け取った2次ユーザは2次暗号鍵を用いて暗号2次著作権データを復号し、利用する。

【0017】

【実施例】以下、図面を用いて本発明の実施例を説明する。初めに、本発明が対象とするデータ著作権管理システムの構成を図1を用いて説明する。図1に示されたシステムはデータベース1、鍵管理センタ2、ユーザ3、3、3・・・およびこれらを相互に接続するネットワークシステム4から構成されている。また、データベース1には情報提供者(Information Provider: IP)5、5、5・・・からデータが供給されるが、場合によってはデータベース1を経由することなく情報提供者6、6、6・・・からネットワークシステム4を経由して直接にユーザ3に対してデータが供給されることがある。なお、本発明において利用するデータはプログラムとデ

ータが組み合わされてオブジェクトである。ユーザ3は単なる利用者ではなく入手した複数の著作権データを組み合わせたり、修正したりすることにより新しい著作物（2次著作物）を提供する情報提供者5あるいは6となる。

【0018】このように構成される本発明のデータ著作権管理システムにおいて、各情報提供者5、6から提供される著作権データは著作権を保護するために暗号化されている。したがって、暗号著作権データを入手したユーザ3が利用するには暗号著作権データを復号する必要がある。そのため、このシステムにおいて暗号鍵はすべて鍵管理センタ2に預けられ、鍵管理センタ2が管理している。また、各情報提供者5、6が採用する暗号方式は自由であるが後で述べる2次利用以降で使用される暗号方式は鍵センタが採用する方式に限られる。

【0019】データベースからのデータ利用は一般的にパーソナルコンピュータを用いて行われるが、そこで用いられるOSとしてはセキュリティ対応処理を組み込んでいるものを使用する必要がある。また、暗号鍵等の管理を行うために著作権管理プログラムが使用されるが、この著作権管理プログラムおよび鍵管理センタ2から受け取った暗号鍵を保管しておく必要があるため、メモリあるいはHDD上にソフトウェア的に実現されあるいは専用のボード、PCカード等でハードウェアとして実現される「キーカード」がこれらの保管場所として用意される。

【0020】鍵管理センタ2は、実際に利用されているか単に登録されているのみで利用されていないかを問わず、データ著作物の著作権の保護と著作権の利用に対する課金を行うために鍵を保管し、保管されている鍵と著作権ラベルの対応付けを行うことにより鍵の管理を行う。

【0021】図2に示されたのは、情報提供者からデータ著作物を入手した1次ユーザが、入手したデータを加工し、加工されたデータを2次利用者へ供給する本発明のデータ著作権処理システム実施例の概要構成である。このシステムにおいては平文1次著作権データD1、暗号1次著作権データ（Encrypted Data）ED1i、平文2次著作権データD2、暗号2次著作権データED2j、平文1次著作権ラベル（Label）LC1、第1暗号鍵（Key）K1iを含む1次利用鍵K1、2次利用鍵K2、第3暗号鍵K3j、平文著作権管理プログラムPCが用いられる。

【0022】このシステムはデータベース11、鍵管理センタ12、1次ユーザ13、2次ユーザ19およびこれらを相互に接続するネットワークシステム14から構成される。また、データベース11には情報提供者15、15、15・・・からデータが供給されるが、場合によってはデータベース11を経由することなく情報提供者16、16、16・・・からネットワークシステム14を経由してあるいは情報提供者16からCDROM

等の情報記録媒体17を介して直接にユーザ13に対してデータが供給されることがある。なお、この図において実線で示されたのは平文データの経路、破線で示されたのは暗号データの経路、点線で示されたのは鍵の経路である。

【0023】このシステムにおいて、平文1次著作権データD1iは第1暗号鍵K1iを用いて暗号化された状態で暗号1次著作権データED1iの形で、

$$ED1i = E(K1i, D1i)$$

10 情報提供者15からデータベース11を介してネットワークシステム14を経由して、情報提供者16からネットワークシステム14を経由してあるいはCDROM等の情報記録媒体17を介して1次ユーザ13に供給される。供給された暗号1次著作権データED1iの利用を希望する1次ユーザ13は、鍵管理センタ12にネットワークシステム14を経由して1次著作権ラベルLC1を提示して1次利用鍵K1の配布を要求する。

【0024】1次ユーザ13からの1次利用鍵K1の配布要求を受けた鍵管理センタ12は提示された1次著作権ラベルLC1により1次利用鍵K1を探し出し、1次利用鍵K1をネットワークシステム14を経由して1次ユーザ13に配布し、このときに課金を行う。1次ユーザ13は配布された1次利用鍵K1に含まれる第1暗号鍵K1iを用いて暗号化1次著作権データED1iを平文化し、

$$D1i = D(K1i, ED1i)$$

利用する。

【0025】平文1次著作権データD1iを1次ユーザ13の装置内へ保存する場合には第1暗号鍵K1iを用いて再暗号化し、

$$ED1i = E(K1i, D1i)$$

暗号化されたデータED1iが保存される。再暗号化されたデータED1iを再利用する場合には第1暗号鍵K1iを用いて再平文化および再暗号化が行われる。

【0026】平文1次著作権データD1iの加工を希望する1次ユーザ13は平文1次著作権データD1iの加工を行うための2次利用鍵K2の配布をネットワークシステム14を経由して鍵管理センタ12に要求する。

【0027】2次利用鍵K2の配布要求を受けた鍵管理センタ12は、2次利用鍵K2をネットワークシステム14を経由して1次ユーザ13に配布する。2次利用鍵K2を受け取った1次ユーザ13は許可鍵の内容に従って平文1次著作権データD1の加工を行い、平文2次著作権データD2jを加工によって得る。平文2次著作権データD2jをユーザ13の装置内に保存する場合には、第2暗号鍵K2によって暗号化される。

$$ED2j = E(K2, D2j)$$

加工が最終的に終了すると、1次ユーザ13は2次著作権データのデータ加工についての2次著作権を行使するために、第3暗号鍵K3jを生成し生成された第3暗号鍵



K3jを鍵管理センタ12に登録する。なお、第3暗号鍵K3jは1次ユーザ13ではなく鍵管理センタ12が作成し、1次ユーザ13からの要求により配布するようにしてもよい。

【0028】1次ユーザ13が平文暗号2次著作権データED2jを外部記憶媒体18への複写あるいはネットワークシステム14を介して転送する場合には、平文2次著作権データED2jを第3暗号鍵で暗号化し、

$ED3j = E(K3j, D2j)$

2次ユーザ19へ供給する。

【0029】供給された暗号2次著作権データED3jの利用を希望する2次ユーザ19は、鍵管理センタ12にネットワークシステム14を経由して第3暗号鍵K3jの配布を要求する。2次ユーザ19からの第3暗号鍵K3jの配布要求を受けた鍵管理センタ12は第3暗号鍵K3jをネットワークシステム14を経由して2次ユーザ19に配布する。第3暗号鍵K3jを受け取った2次ユーザ19は、第3暗号鍵K3jを用いて暗号2次著作権データED2jを復号し、

$D2j = D(K3j, ED2j)$

利用する。その場合も、暗号化データED2jを再度利用する場合には第3暗号鍵K3jを用いて復号化および暗号化が行われる。

【0030】1次著作権データの入手、1次著作権データの1次利用、1次著作権データの加工、加工された2次著作権データの供給および2次著作権データの利用について詳細に説明する。このシステムにおいて、複数の1次著作権データD1iは1次暗号鍵K1iを用いて暗号化された状態で

$ED1i = E(K1i, D1i)$

平文1次著作権ラベルLC1とともに、情報提供者11から直接にあるいはデータベースを介して、1次ユーザ13に供給される。

【0031】著作権管理プログラムPCはユーザによる著作権データの使用を管理するものであり、具体的には与えられた暗号鍵を用いての著作権データの復号化及び再暗号化および利用鍵の内容に従う著作権データの利用制限を行う。このシステムにおいて提供される暗号データED1jには暗号鍵入手等に利用するための平文の1次著作権ラベルLC1が付けられており、すなわち、暗号1次著作権データED1は平文1次著作権ラベルLC1と暗号1次著作権データED1iから構成されている。平文1次著作権ラベルLC1にはデータのタイトル名、使用しているアプリケーション・プログラム名、1次著作権者名が記入されている。供給された暗号1次著作権データED1iの利用を希望する1次ユーザ13は、鍵管理センタ12にネットワークシステム14を経由して平文1次著作権ラベルLC1を提示して1次利用鍵K1の配布を要求する。

【0032】提示された1次著作権ラベルLC1により、

配布すべき1次利用鍵が鍵K1であることを確認した鍵管理センタ12は確認された1次利用鍵K1をネットワークシステム14を経由して1次ユーザ13に配布する。配布された1次利用鍵K1を受信した時点で1次ユーザ13の装置は著作権管理モードになり、1次ユーザ13は1次著作権データの利用が可能になる。なお、第1暗号鍵K1iは1次利用鍵K1に含まれているため、1次ユーザ13から第1暗号鍵K1iは認識されない。一方、鍵管理センタ12は課金処理を行うとともに著作権データの使用状況および1次ユーザ13のデータベース利用状況を把握する。

【0033】図3に示されたのは、本発明において著作権管理プログラムPCが行う1次利用の制限を説明する概念図である。先願である特願平6-64889号に記載された発明と同様に、本願発明のデータ著作権管理システムにおける入手したデータの1次利用は通常の利用形態すなわちデータの直接的な利用およびその利用結果の印刷を含む出力に限定され、外部記憶媒体への複写あるいはネットワークシステムを経由しての転送及び加工、さらに原則としてデータの装置内部での保存を行うことはできない。ただし、データが暗号化されている場合には保存は可能である。なお、使用中のアプリケーション・プログラムにより著作権データ以外のデータDを表示・印刷・保存・複写・加工・転送することが可能なことはいうまでもない。

【0034】この図において21は1次ユーザの装置20内に内蔵された不揮発性半導体メモリあるいはハード・ディスク・ドライブ等の記憶装置、22は出力用の表示装置、23は出力用の印刷装置、D1は1次著作権データ、Dは一般データ、24はフレキシブルディスクあるいはCDROMによる複写、ネットワークシステムによる転送でデータを供給される2次ユーザである。なお、この図において実線で示されたのは許される処理経路、点線で示されたのは許されない処理経路である。

【0035】1次ユーザ13が外部の情報提供者15あるいは16から、直接にあるいはデータベース11を介して入手した暗号1次著作権データED1iはともに供給される平文1次著作権ラベルLC1と組み合わせられて1次ユーザ装置20の記憶装置21に格納される。記憶装置21に格納されている暗号1次著作権データED1iの1次利用を希望する1次ユーザ13は著作権管理プログラムPCにより暗号1次著作権データED1iの概要説明および暗号1次著作権データED1iが使用しているアプリケーション・プログラムの情報等が表示された平文1次著作権ラベルLC1を参照し、暗号著作権1次データED1i作成に使用されているアプリケーション・プログラムの有無等この暗号著作権1次データED1iの使用環境を確認する。

【0036】その結果、暗号著作権1次データED1iの利用が可能であると判断され、1次利用者13がこの暗



号1次著作権データED1iを使用することを著作権管理プログラムPCに入力すると、著作権管理プログラムPCは暗号1次著作権データED1iが使用しているアプリケーション・プログラムを起動し、暗号1次著作権データED1iを記憶装置21から装置内のメモリに読み込む。その一方、平文1次著作権ラベルLC1が鍵管理センタ12に送られ、その結果、前に述べた処理フローにしたがい1次利用鍵K1が供給されると、1次利用鍵K1に含まれている1次暗号鍵K1iを用いて暗号1次著作権データED1iが平文1次著作権データD1iに平文化され、D1i=D(K1i, ED1i)起動されたアプリケーション・プログラムによって使用することが可能となる。

【0037】装置20のメモリ上の平文1次著作権データD1iを記憶装置21に保存する場合には第1暗号鍵K1iを用いて暗号化して、

$ED1i = E(K1i, D1i)$

保存が行われる。この保存には、データ保全のための一時的ファイル(Temporary File)の作成・保存も含まれる。再暗号化されたデータED1iを再利用する場合には第1暗号鍵K1iを用いて再復号化および再暗号化が行われる。なお、平文1次著作権データD1あるいは暗号1次著作権データED1iの表示・印刷、保存あるいは加工以外の利用形態すなわち外部記憶媒体への複写および他の装置への転送は著作権管理プログラムPCにより禁止される。

【0038】前に述べたように本発明のデータ著作権管理システムにおいて、入手した著作権データは通常の利用形態すなわちデータを表示装置22に表示することによって直接的な利用を行うことおよびその利用結果をプリンタ23で出力することに限定され、外部記憶媒体への複写あるいはネットワークシステムを経由しての2次ユーザ24への転送および加工を行うことはできない。したがって、1次著作権データD1iの1部を切り出して他のデータDに張り付けること(Cut & Paste)および他のデータDの1部を切り出して1次著作権データD1iに張り付けることは著作権管理プログラムによって禁止される。また、1次著作権データD1iは第1暗号鍵K1iを用いて暗号化された状態ならば例外的に記憶装置21に保存することができるが、何らかの加工が行われた場合に保存は禁止される。

【0039】本発明のデータ著作権管理システムにおいて、1次著作権データD1と一般データDとの区別および著作権データが加工されたか否かは、著作権管理プログラムPCが判別する。コンピュータファイルはファイル本体とそのファイルの属性を記述した管理テーブルから構成されている。したがって、この管理テーブルを調べることによりそのファイルが著作権データであるか否かが判別される。また、この管理テーブルにはファイルサイズ、作成日付が記入されており、これらを調べるこ

とによりファイルの加工が行われたか否かが判別される。

【0040】記憶装置21に保存されているときに1次著作権データD1iは暗号化されて1次著作権ラベルLC1と結合されているが、メモリ上に読み込まれたときには著作権管理プログラムにより1次著作権データD1iと1次著作権ラベルLC1は分離され、分離された著作権ラベルLC1は著作権管理プログラムPCにより管理される。著作権管理プログラムPCは1次著作権データD1iがどのアプリケーション・プログラムによって使用されているかを監視し、1次著作権データD1iの一般データDへの切り出し/張り付けおよび一般データDの1次著作権データD1iへの切り出し/張り付けが行われることを禁止する。

【0041】図4に示されたのは、本発明において著作権管理プログラムPCが行うデータ加工利用の制限を説明する概念図である。1次利用の結果、平文1次著作権データD1iの加工を行うことが適切であると判断されたとき、1次ユーザ13は平文1次著作権データD1iの加工を行うことをネットワークシステム14を経由して鍵管理センタ12に対して通知する。

【0042】平文1次著作権データD1iの利用を希望する1次ユーザ13は平文1次著作権データD1iの加工を行うための2次利用鍵K2の配布をネットワークシステム14を経由して鍵管理センタ12に要求する。2次利用鍵K2の配布要求を受けた鍵管理センタ12は2次利用鍵K2をネットワークシステム14を経由して1次ユーザ13に配布する。このことにより1次ユーザ13の装置20は加工モードになり、1次ユーザ13は1次著作権データの加工が可能になる。

【0043】1次ユーザ13は暗号1次著作権データED1iを第1暗号鍵K1iで平文1次著作権データD1iに平文化した上で表示装置23に表示してデータの加工を行うが、初めに1次著作権データの著作権を保護するために加工用平文1次著作権データD1iの複写が行われ、この複写によって得られた加工用平文1次著作権データD1i'に対して加工が行われる。この加工用平文1次著作権データD1i'あるいはこの加工途中の平文1次著作権データD1i''をユーザ13の装置内に保存する場合には2次利用鍵K2により暗号化されて、

$ED1i' = E(K2, D1i')$

または  $ED1i'' = E(K2, D1i'')$

保存が行われる。暗号1次著作権データED1iは加工されることなく記憶装置21内に保存されており、その管理テーブルと加工された加工用平文1次著作権データD1i'あるいはD1i''のファイルサイズ、作成日付を調べることによりそのファイルが加工されたファイルであるか否かが判別される。

【0044】データの加工が終了するとそのデータは新規な複数の平文2次著作権データD2jとなり、これらの

データD2jについて新たに2次著作権が発生する。この2次著作権を保護するために平文1次著作権D1を加工した1次ユーザ13は鍵管理センタ12に対して第3暗号鍵K3jの配布を要求し、第3暗号鍵K3jの配布要求を受けた鍵管理センタ12は、第3暗号鍵K3jをネットワークシステム14を経由して1次ユーザ13に配布する。第3暗号鍵K3jの配布を受けた1次ユーザ13は、この第3暗号鍵K3jを用いて平文2次著作権データD2jを暗号化し、

$ED2j = E(K3j, D2j)$

1次ユーザ13の記憶装置21内には暗号化データED2jが保存される。この暗号化データED2jを利用する場合には第3暗号鍵K3jを用いて復号化および暗号化が行われる。

【0045】1次ユーザ13により加工された平文2次著作権データD2jには、情報提供者が有する加工される前の平文1次著作権データD1iの1次著作権に加えて、データ加工についての2次著作権が存在する。この2次著作権を行使するために1次ユーザ13は鍵管理センタ12に3次暗号鍵K3jとともに、データのタイトル名、使用しているアプリケーション・プログラム名、内容概要、1次著作権者名を送り、鍵管理センタ12は3次暗号鍵K3jとともに保管し、管理する。

【0046】一方、1次ユーザ13は暗号化された2次著作権データED2jを外部記憶媒体18への複写あるいはネットワークシステム14を介して転送することにより2次ユーザ24へ供給する。

【0047】供給された暗号2次著作権データED2jの利用を希望する2次ユーザ24は、鍵管理センタ12に3次暗号鍵K3jの配布を要求する。この3次暗号鍵K3jによる平文2次著作権データD2jの利用は平文2次著作権データD2jの一般的な利用及びユーザ装置内への保存に限定され、平文2次著作権データD2jあるいは暗号化2次著作権データED2jの外部記憶媒体18への複写あるいはネットワークシステム14を利用することによる3次ユーザへの転送及び平文2次著作権データD2jの加工を行うことはできない。

【0048】前に述べたように、本発明において扱う著作権データはプログラムとデータが一体化した「オブジェクト」を対象としており、このオブジェクトはコンピュータプログラミングあるいは各種処理において部品の取り扱いをすることができる。図5および図2により、オブジェクトである複数の著作権データを利用して新しい著作権データを作る場合について説明する。図5において、31、32、33は各々オブジェクトとして構成された著作権データD11、D12、D13であり、これらの著作権データD11、D12、D13を利用して新しい著作権データD2j30が作成される。著作権データD11、D12、D13の利用形態としては、34に示された著作権データD11のようにその全部を利用する、35に示され

た著作権データD12のようにその一部を利用するあるいは36に示された著作権データD13のように修正して利用する、の3形態がある。

【0049】著作権データの加工は、オブジェクト単位で著作権データをリンクして引用して重ね合わせ/組み合わせを行うことにより加工処理が行われ、このような重ね合わせおよび組み合わせは自由に行うことができる。

また、このように重ね合わせ/組み合わせが行われた著作権データ37にさらに他の事項を付け加えることもできる。このようにして新規に作成された著作権データD2jはオブジェクトの集合体として構成されている。

【0050】このようにして作成された平文2次著作権データD2jには1次著作権データD1iの著作権の他に新たに加工を行った1次ユーザ13の2次著作権が発生する。この2次著作権を行使するためには平文2次著作権データの暗号化が必要であり、そのために1次ユーザ13は3次暗号鍵K3jを用意し、平文著作権データD2jを3次暗号鍵K3jを用いて暗号化し、

$ED2j = E(K3j, D2j)$

外部記憶媒体18への複写あるいはネットワークシステム14を介して転送することにより2次ユーザ19へ供給する。また、3次ユーザが3次暗号鍵K3jを容易に入手することができるように、鍵管理センタ12に第3暗号鍵K3jを登録する。この第3暗号鍵K3jの登録により、1次ユーザ13の2次著作権が鍵管理センタ12に記録される。

【0051】このとき1次ユーザ13から鍵管理センタ12に送られるのは、作成した複数の2次著作権データの数に対応した複数の第3暗号鍵K3jの他に、第3暗号鍵K3jの数、2次暗号鍵K2i、使用した1次著作権データ、著作権管理プログラムがリンクしている他の著作権データの情報、使用した著作権データへのアクセスパス、使用した著作権データが使用しているアプリケーションプログラムおよび著作物説明文章等である。

【0052】供給された暗号2次著作権データD2jの利用を希望する2次ユーザ19は、鍵管理センタ12に第3暗号鍵K3jの配布を要求する。第3暗号鍵K3jの配布要求を受けた鍵管理センタ12は、第3暗号鍵K3jをネットワークシステム14を経由して2次ユーザ19に配布する。第3暗号鍵K3jを受け取った2次ユーザ19は、第3暗号鍵K3jを用いて暗号2次著作権データED2jを復号・平文化し、利用する。

【0053】著作権管理プログラムPCは、第3暗号鍵K3jを受け取ると、それぞれの著作権データD2jに著作権ラベルLC2jを付けて2次利用者が利用可能な状態にする。この時、新規作成の著作権データとリンクされていたオブジェクトである著作権データとのリンクが解除される。解除された時点で、リンク関係だけであった利用著作権データの実体が、新規著作権データED2jに埋め込まれ、ED2jファイルだけで著作物の流通が可能と

なる。この場合も、暗号著作権データED2jを再度利用  
 する場合には第3暗号鍵K3jを用いて復号化および暗  
 号化が行われる。

【0054】鍵管理センターは、第3暗号鍵K3jを要  
 求元に返送するとともに、著作権ラベルLC1及びLC2を  
 もとに課金処理を行う。著作権データ所有者は、鍵管理  
 センターに申請することにより自分の著作権データのアク  
 セスパスを変更することができる。著作権データの所  
 有者は、第3暗号鍵K3jで自分の著作権データを加工  
 （修正）することも可能であり、さらに、別の鍵で登録  
 することも可能である。

#### 【図面の簡単な説明】

【図1】本発明が対象とするデータ著作権管理システム  
 の構成図。

【図2】本発明のデータ著作権処理システム実施例の概  
 要構成図。

【図3】本発明において著作権管理プログラムPCが行  
 う1次利用の制限を説明する概念図。

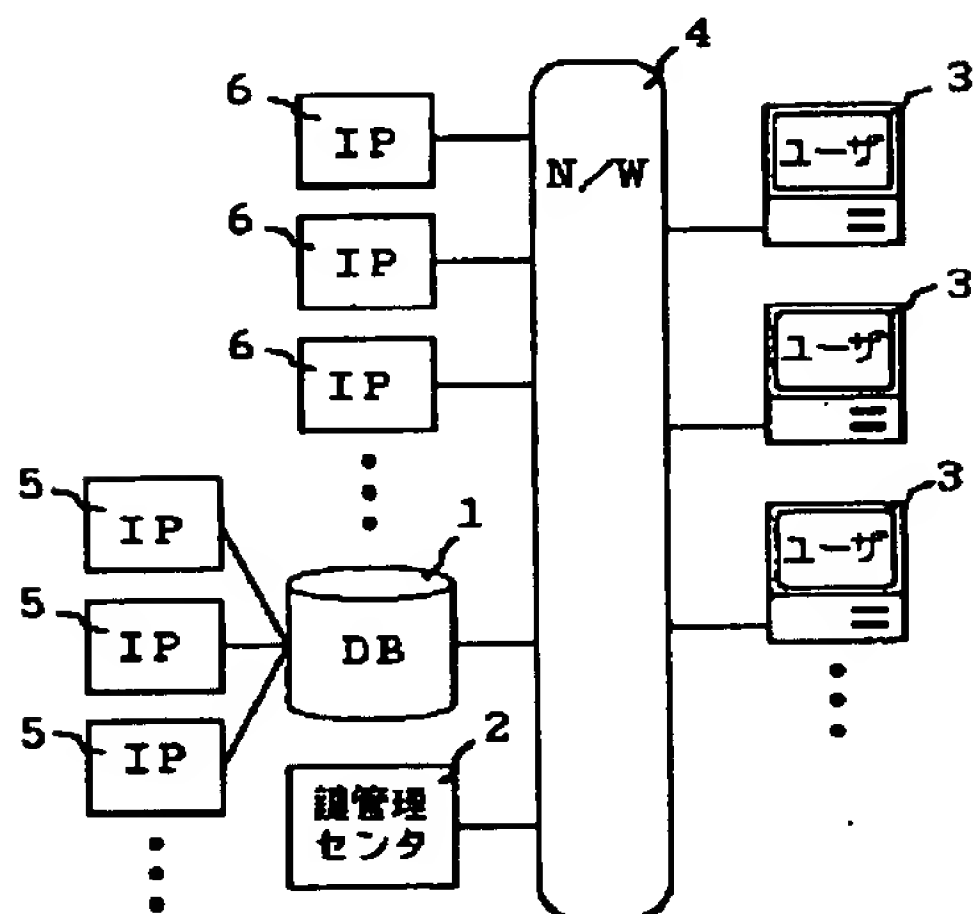
【図4】本発明において著作権管理プログラムPCが行  
 うデータ加工利用の制限を説明する概念図。

【図5】オブジェクトである複数の著作権データを利用  
 しての新しい著作権データ作成の説明図。

#### 【符号の説明】

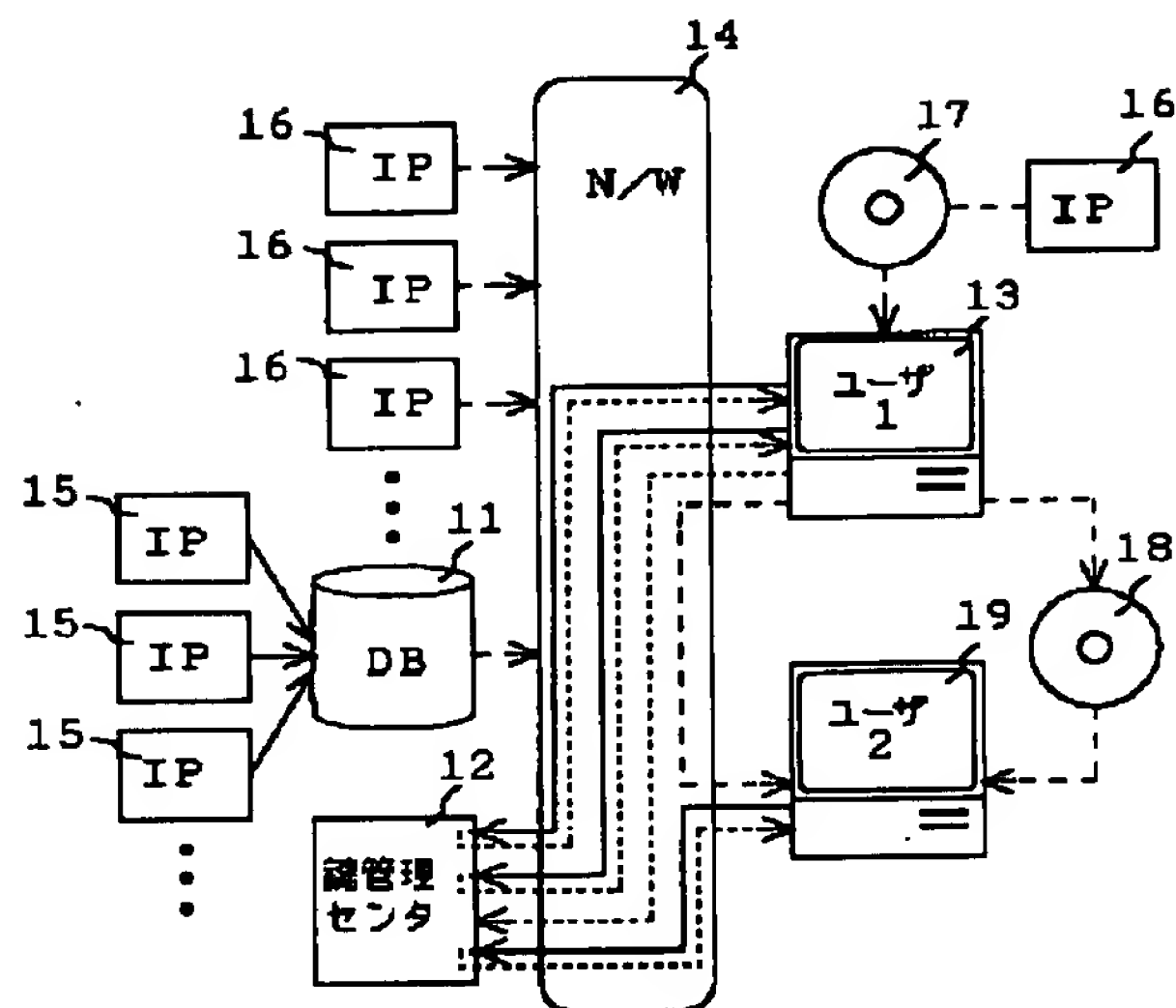
- 1, 11 データベース
- 2, 12 鍵管理センタ
- 3 ユーザ

【図1】

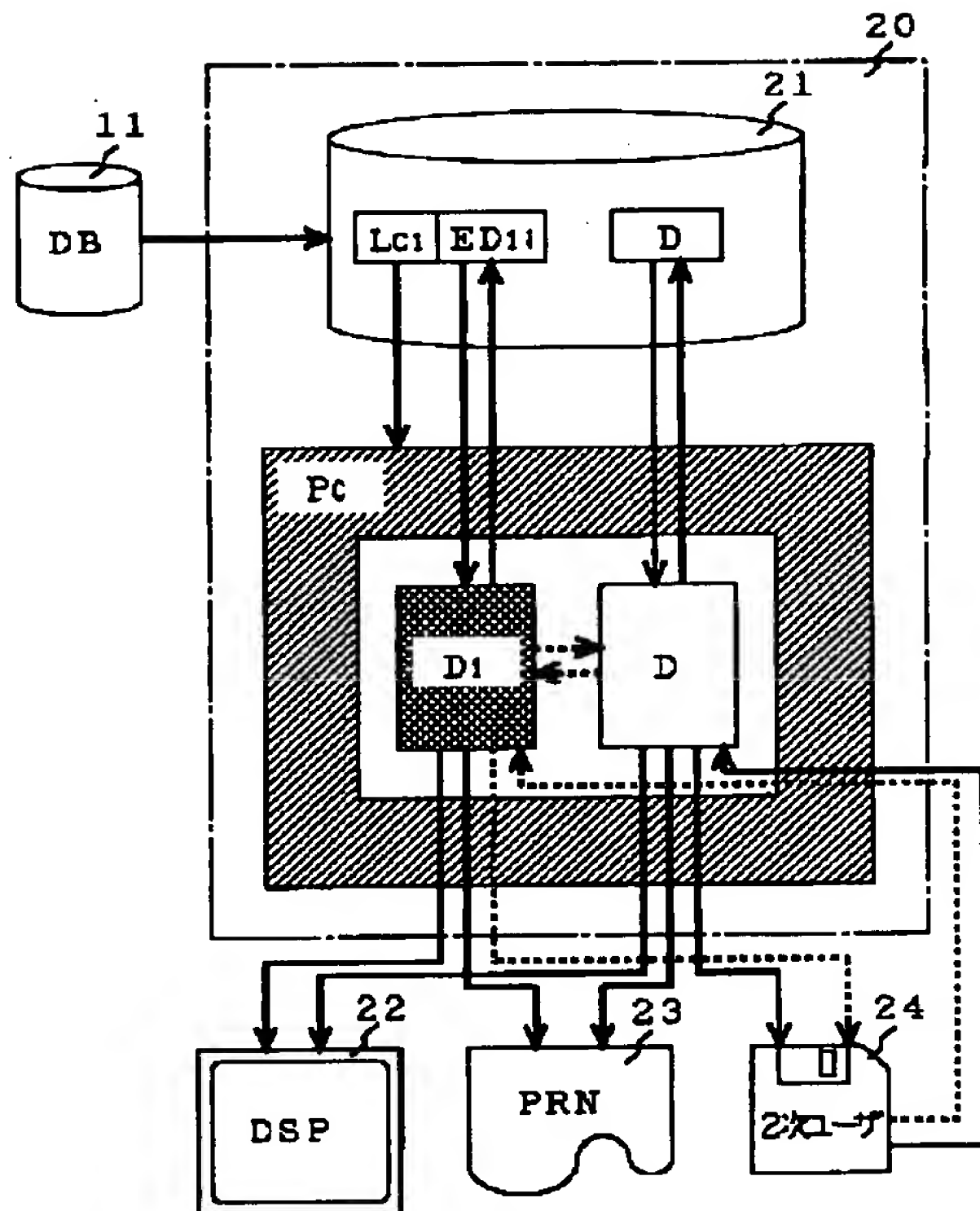


- 4 ネットワークシステム
- 5, 6, 15, 16 情報提供者
- 11 データベース
- 12 鍵管理センタ
- 13 1次ユーザ
- 14 ネットワークシステム
- 17 情報記録媒体
- 18 外部記憶媒体
- 19, 24 2次ユーザ
- 20 1次ユーザの装置
- 21 記憶装置
- 22 表示装置
- 23 印刷装置
- 24 2次ユーザ
- 30 新しい著作権データ
- 31, 32, 33 著作権データ
- D 一般データ
- D1 1次著作権データ
- D1i 平文1次著作権データ
- D1i' 加工用平文1次著作権データ
- D2j 平文2次著作権データ
- ED1i 暗号1次著作権データ
- ED2j 暗号化データ
- K1i 第1暗号鍵
- K3j 第3暗号鍵
- PC 著作権管理プログラム

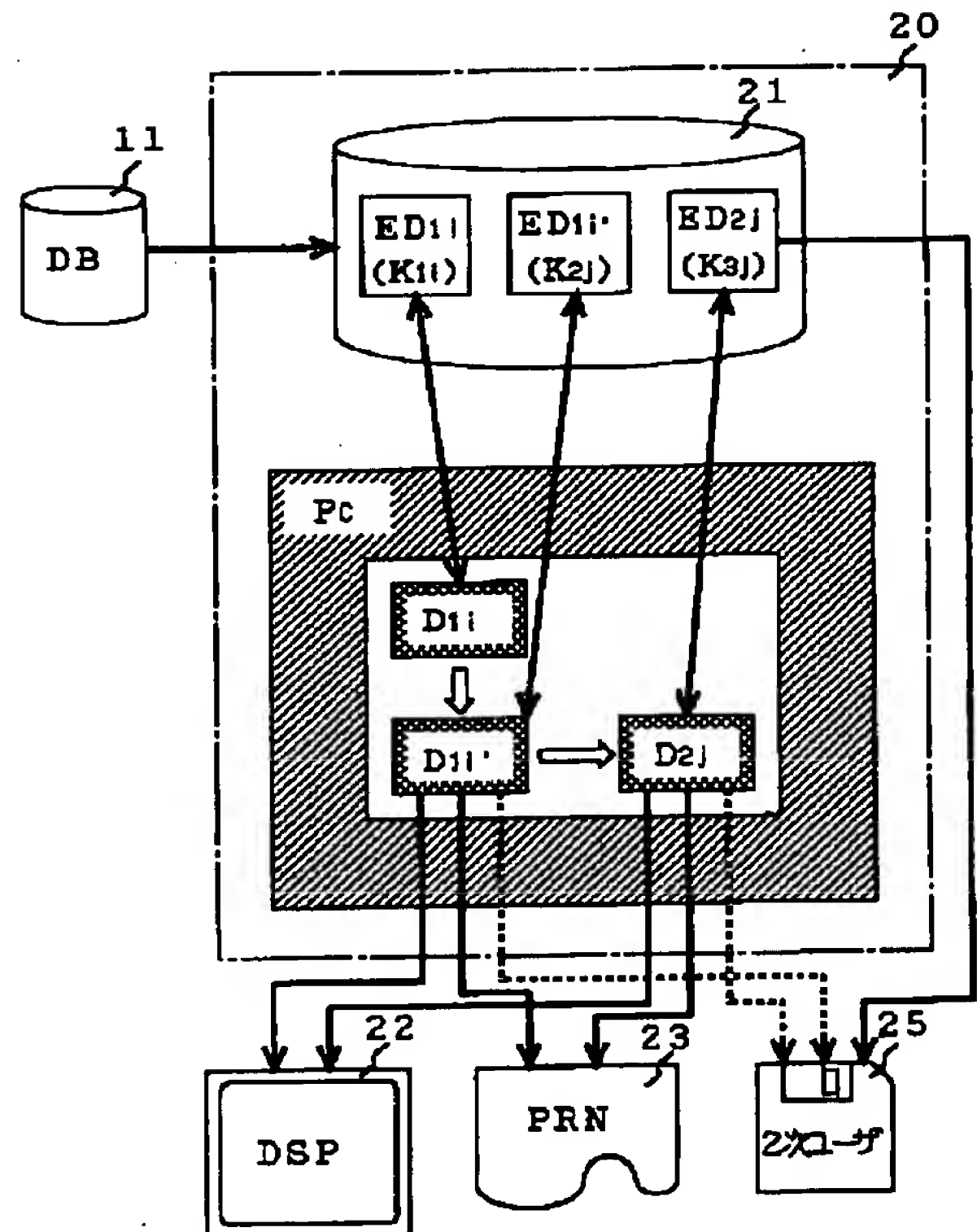
【図2】



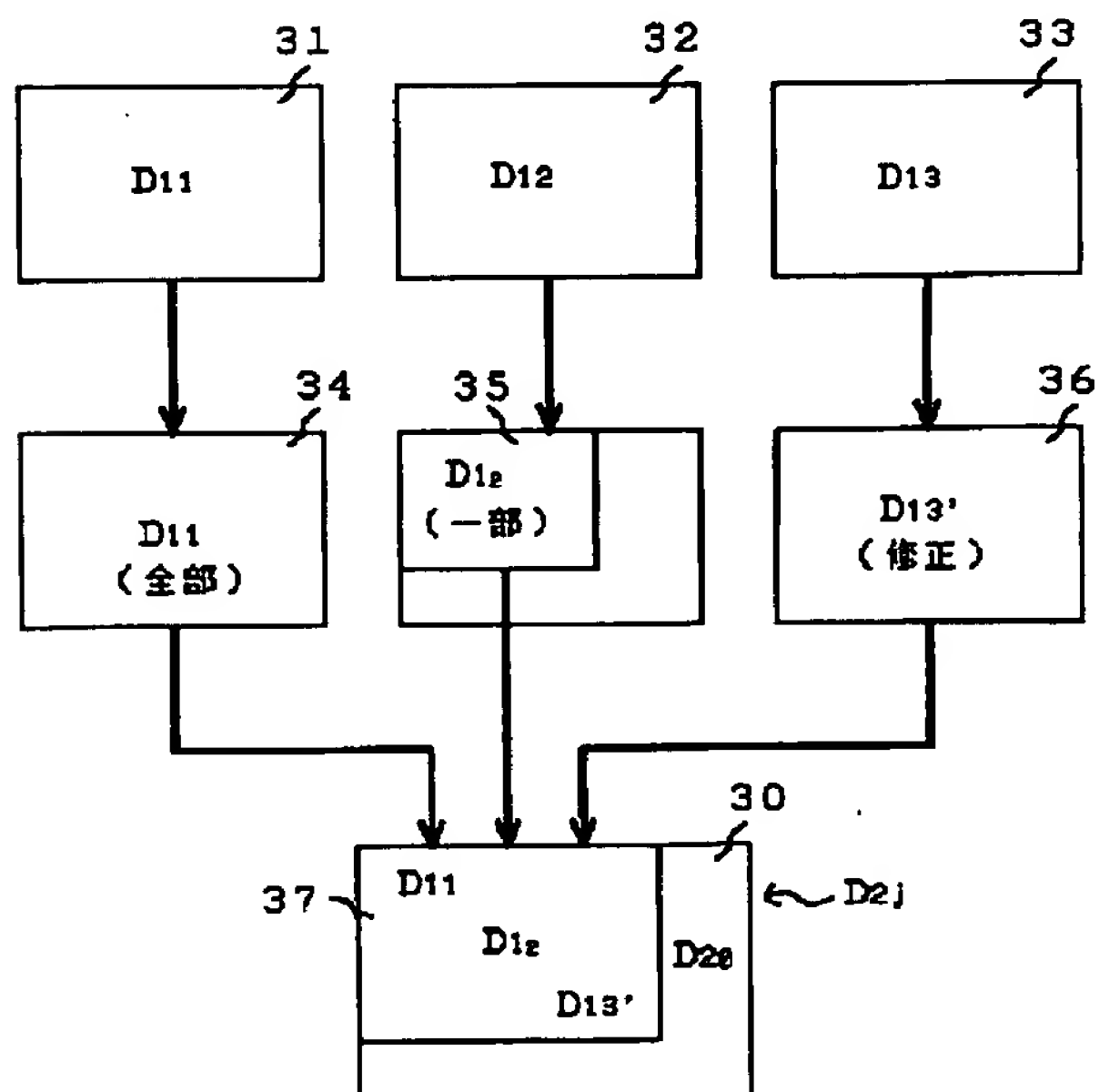
【図3】



【図4】



【図5】





フロントページの続き

(51)Int.Cl. <sup>6</sup>	識別記号	序内整理番号	F I	技術表示箇所
H O 4 L 9/14			H O 4 N 7/167	
H O 4 N 7/167				

(43)公開日 平成8年(1996)10月1日

(51) Int. Cl. <sup>8</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0	9364-5L	G 0 6 F 15/00	3 3 0 A
3/14	3 5 0		3/14	3 5 0 A

審査請求 未請求 請求項の数9 OL (全 15 頁)

(21)出願番号 特願平7-261144

(22)出願日 平成7年(1995)10月9日

(31)優先権主張番号 3 2 1 6 4 4

(32)優先日 1994年10月11日

(33)優先權主張国 米国 (US)

(71)出願人 390009531

インターナショナル・ビジネス・マシーンズ・コーポレーション

INTERNATIONAL BUSINESS  
MACHINES CORPORATION

アメリカ合衆国10504、ニューヨーク州  
アーモンク (番地なし)

(72)発明者 マーク・アーウィン・カーソン

アメリカ合衆国20953 メリーランド州ロ  
ックヴィル ジュディス・ストリート  
4317

(74)代理人 弁護士 合田 潔 (外2名)

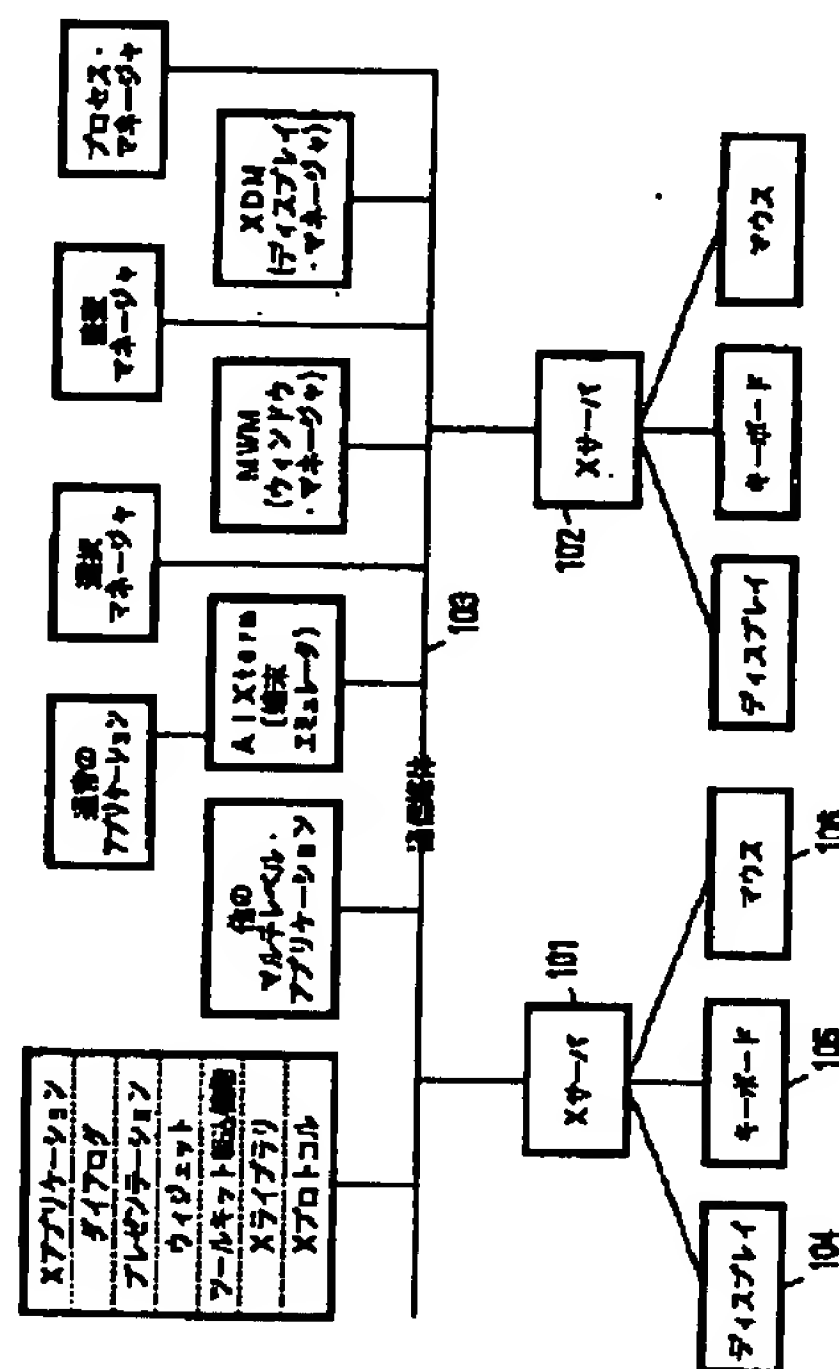
**最終頁に続く**

(54) 【発明の名称】 安全なデータ転送を行うための方法および機密レベル変更選択機構

(57) 【要約】 (修正有)

【課題】 未承認のウィンドウ・システム・クライアント・プログラムが選択マネージャという特殊承認クライアント・プログラムによって仲介されてユーザの制御下で安全保護領域間でデータを転送できるようにする。

【解決手段】 使用する機構は、機密レベル変更カット・アンド・ペースト操作に関するコンパートメント化モード・ワークステーション（CMW）要件の機能を満たすように構成することができる。CMWのカット・アンド・ペースト要件を満たし、機密レベル変更選択機構が抜け道として機能するのを防止するため、この機密レベル変更選択機構では、必須アクセス管理（MAC）上位移行操作中の低レベル・プロセスへの通信にダミー・ウィンドウIDを使用し、すべての機密レベル変更操作について、転送の続行を許可する前にユーザ確認を要求するポップアップを表示するよう選択マネージャに指示する。この選択機構は、カット・アンド・ペースト用の構成可能な機密レベル変更選択操作をサポートする。



## 【特許請求の範囲】

【請求項1】安全なウィンドウ・システム用の機密レベル変更選択機構において、

前記ウィンドウ・システム上の個別のウィンドウで動作し、それぞれがそのウィンドウ内にデータを表示する、複数のクライアント・プログラムと、

あるクライアント・プログラム・ウィンドウから別のクライアント・プログラム・ウィンドウにデータを転送するためのカット・アンド・ペースト操作の選択マネージャというクライアントとを含み、前記選択マネージャがコンパートメント化モード・ワークステーション (CMW) 要件を満たし、状態の変化をアプリケーションに通知するためにアプリケーションに事象を送信し、前記選択マネージャが転送中のデータの所有権およびその他の安全保護プロパティを操作して、制御式検査可能データ転送の実行を可能にすることを特徴とする、機密レベル変更選択機構。

【請求項2】必須アクセス管理 (MAC) 上位移行操作中の低レベル・プロセスへの通信時に、前記ウィンドウ・システムがダミーのウィンドウ ID を使用することを特徴とする、請求項1に記載の機密レベル変更選択機構。

【請求項3】すべての機密レベル変更操作について、選択項目が転送される前に前記ウィンドウ・システムが前記選択マネージャに事象を送信し、その結果、転送続行が許可される前にユーザ確認を要求するポップアップを選択マネージャが表示することを特徴とする、請求項1に記載の機密レベル変更選択機構。

【請求項4】安全なウィンドウ・システム内で安全保護属性を有するデータを安全に転送する方法において、データへのアクセスに関する事前定義安全保護レベルを有する要求側からデータ転送に関する要求をウィンドウ・システムが受け取るステップと、

要求側によって指定されたウィンドウ ID とプロパティ ID が選択側所有者から隠されて、要求側が必須アクセス管理 (MAC) 上位移行時に低レベル・プロセスと通信するときに選択項目の所有者が要求側に関する安全保護関連情報を入手できないようにするために、特殊なウィンドウが選択項目所有者からアクセス可能になる、前記ウィンドウ・システム上で動作する選択マネージャというクライアント・プログラムが、選択項目所有者の安全保護属性を継承する特殊なウィンドウとプロパティを作成するステップとを含むことを特徴とする、安全なデータ転送方法。

【請求項5】前記選択項目所有者が前記選択マネージャに選択項目データを転送するステップであって、転送が完了するまで前記選択マネージャがデータの所有者になり、それに対する排他的権利を有するステップと、前記選択項目所有者から選択項目要求側に転送されるデータをログイン・ユーザが検査できるようにし、機密レ

ベル変更操作について、データ転送の続行が許可される前にユーザ確認を要求するユーザ・インタフェースを提供するステップとをさらに含むことを特徴とする、請求項4に記載の安全なデータ転送方法。

【請求項6】MAC下位移行の使用にかかわる操作を試みた場合およびデータ転送および再分類にかかわる安全保護違反を犯した場合に監査事象を生成するステップをさらに含むことを特徴とする、請求項5に記載の安全なデータ転送方法。

10 【請求項7】要求側のウィンドウとプロパティに対する任意アクセス制御 (DAC) 書込みアクセス制限を指定変更するために十分な特権を有する選択機構を提供するステップをさらに含むことを特徴とする、請求項6に記載の安全なデータ転送方法。

【請求項8】選択項目要求側と選択項目所有者との間で安全なウィンドウ・システム内で安全保護属性を有するデータを安全に転送する方法において、

前記選択項目要求側がウィンドウ・システムを動作させる選択マネージャというクライアントに転送される要求を出すステップと、

20 前記選択マネージャが必須アクセス管理 (MAC) ダイアログと任意アクセス制御 (DAC) ダイアログを表示するステップと、

後で選択項目の所有者が選択項目をポストすることができ、専用のウィンドウ上で前記選択マネージャがプロパティを作成し、選択項目要求を生成し、最初に意図した受信側として前記選択項目所有者に前記選択項目要求を送信するステップと、

30 前記選択項目要求に応答して、前記選択項目所有者が前記選択マネージャのプロパティ上で選択項目データをポストし、前記選択マネージャに選択通知事象を出すステップと、

ユーザが未修正通過の要求を許可するか、要求を取り消すか、または転送中のデータを下位移行できるように、前記選択項目所有者から前記選択項目要求側に渡されるデータをユーザが検査できるようにするステップと、ユーザが要求を取り消した場合に監査事象を生成するステップと、

40 前記選択マネージャがそれ自体のウィンドウ／プロパティから前記選択項目要求側のウィンドウ／プロパティに選択項目データを転送し、そのプロパティ上の前記選択項目の可用性に関する通知を要求側に出すステップと、前記選択項目要求側がデータを読み取り、前記選択マネージャに通知を出すステップと、

前記選択マネージャがデータ転送の完了を所有者に通知するステップとを含むことを特徴とする、安全なデータ転送方法。

50 【請求項9】前記選択マネージャによる前記転送ステップが増分式に実行され、それぞれの転送ごとに個別にレベルを付けるかどうかを指定するようユーザに要求する

ステップをさらに含むことを特徴とする、請求項8に記載の安全なデータ転送方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、一般的に、コンピュータ・ウィンドウ・システム内でのカット・アンド・ペースト操作によるデータ転送に関し、より詳細には、未承認ウィンドウ・システム・クライアント・プログラムが特殊なクライアント・プログラムによって仲介される転送によってユーザの制御下でユーザの示唆により安全保護領域間でデータを転送できるようにするための安全な手段に関する。

【0002】

【従来の技術】コンピュータ・システムでは、ユーザにグラフィカル・ユーザ・インタフェース（GUI）を提供してマルチタスクのコンピュータ・プログラムを管理するために、ウィンドウ・システムが一般に使用されている。通常、コンピュータ上で現在実行されているコンピュータ・プログラムごとに別々のウィンドウがオープンされる。とりわけ、ウィンドウ・システムは、あるプログラムが作成したある文書から別の無関係のプログラムが作成した別の文書へのデータ転送を容易にするためのいくつかのツールをユーザに提供する。このようなツールの1つは、あるウィンドウでデータを囲み、それを別のウィンドウに移動して挿入する、いわゆる「カット・アンド・ペースト」操作である。この操作は通常、マウスで制御したカーソルを使用して実施される。現在使用されているウィンドウ環境の1つは、AT&T Bell Laboratories社が開発したUNIXオペレーティング・システム（UNIXはNovell社の商標である）上で動作する「Xウィンドウ・システム」（Massachusetts Institute of Technologyの商標）である。

【0003】安全保護レベルは、Defence Intelligence Agency（DIA）の"Requirements for System High and Compartmented Mode Workstations"（CMW規定という）の基本要件の1つである。この規定では、特に、安全保護が異なる可能性のある複数のウィンドウをいつでもオープンできるような、ワークステーション用の安全なマルチレベル・ウィンドウ・システムを扱っている。このようなウィンドウの安全保護レベルは、安全保護レベル、すなわち、1つの主題またはオブジェクトに関連する全体的な機密レベルを示す必須アクセス管理（MAC）ラベルと、データの集合体にラベルを付ける情報ラベルという、より細分性の高いラベルとによって管理される。機密レベルまたはMACレベルは、特権ユーザを除くすべてのユーザ向けの「上位読取りなし」（より高い機密レベルでのオブジェクトの読取りなし）規則および「下位書込みなし」（より低い機密レベルでのオブジェクトの書込みなし）規則で実施される。この「上位読取りなし」規則のため、通常のユーザはできるだけ高い

機密レベルで作業する傾向があり、そのため、何でもみられるようになっている。しかし、「下位書込みなし」規則では、その内容がどんなにつまらないものでもすべてのオブジェクトに同一の高い機密レベルでラベルを付けなければならない。このようなデータの過剰分類を防止するため、CMWは、データの「真」の機密性のある程度を示す、情報ラベルのシステムを提供している。情報ラベルはユーザ制御とシステム制御の両方があり、ユーザは最初に情報ラベルを設定し、必要に応じて変更することができ、システムは伝播または浮動によりそれを更新する。すなわち、プロセスが機密データを読み取ると、それ自体の（プロセス）情報ラベルがそれが読み取ったすべてのデータの情報ラベルの最大値（最小上限）まで浮動し、その後それが他のオブジェクトに書き込むときには、そのオブジェクトがデータを受け取ることができる想定して、そのオブジェクトの情報ラベルが同様に浮動する。

【0004】機密ラベルと情報ラベルの機密レベルが異なるときにデータのウィンドウ間移動を行うことは、CMWを有用にする基本的特徴の1つである。しかし、すべてのウィンドウ間移動は、前述の「上位読取りなし、下位書込みなし」の規則に適合しなければならない。具体的には、カット・アンド・ペースト操作によるラベルの機密レベル変更は、次のように行うことができる。MACラベルの上位移行はすべての特権ユーザと通常ユーザが行うことができ、MACラベルの下位移行は特権ユーザのみ行うことができ、情報ラベルの上位移行または下位移行はすべての特権ユーザと通常ユーザが行うことができる。CMWでは、ユーザがすべてのラベル変更を認識するように、これを対話式に行うよう要求している。

【0005】Xウィンドウ・システムは、1台のXサーバと、様々な機能を実行する複数のアプリケーション・プログラムから構成される。Xサーバは、ユーザ入力の結果として生成される事象の送信により、このようなアプリケーションとやりとりする。Xウィンドウ・システムでは、Xサーバは、Xtermなどの通常は未承認のクライアント・プログラムによって開始され制御される、カット・アンド・ペースト操作を仲介するだけである。カット・アンド・ペースト操作に直接かわるもう1つのアプリケーションは、ウィンドウ・マネージャである。ウィンドウ・マネージャは、ウィンドウの視覚的操作のほとんどを担当する。

【0006】SecureWareは、ベースとしてXウィンドウ・システムを使用する市販のCMWを備えているが、カット・アンド・ペースト操作には個別のクライアントではなくウィンドウ・マネージャを使用する。SecureWareのインプリメンテーションでは、所与のデータ・タイプしか扱うことができず、クライアントは、承認後のデータの変更や承認前のデータの受信を内密に行う可能性が



ある。専用の文書以外には、その作業を詳述した文書が発行されておらず、特に、カット・アンド・ペースト操作に関する処理方法については何も発行されていない。Smith他は"Secure Multi-Level Windowing in a B1 Certifiable Secure UNIX Operating System" (Winter 1989 USENIX Conference Proceedings) において、ウィンドウ上でのカット・アンド・ペースト操作について記述しているが、この研究はXウィンドウ・システムに基づくものではなく、単にMAC準拠に関連しているだけである。情報ラベルの概念はまったく示されていない。Carson他は"From B2 to CMW: Building a Compartmented Mode Workstation on a Secure Xenix Base" (Proceedings of the AIAA/ASIS/IEEE Third Aerospace Computer Security Conference, 1987) において、CMWインプリメンテーションの1つについて記述しているが、このインプリメンテーションでは、そのオペレーティング・システムとしてXENIXを、そのベース・ウィンドウ・システムとしてViewnixを使用し、カット・アンド・ペースト操作では完全に中央制御下にあるまったく異なる機構を使用している。(XENIXはマイクロソフト社の商標であり、ViewnixはFive Paces Software社の商標である。)

#### 【0007】

【発明が解決しようとする課題】したがって、本発明の目的は、未承認ウィンドウ・システム・クライアント・プログラムが選択マネージャという特殊な承認クライアント・プログラムによって仲介された転送によってユーザの制御下でユーザの示唆により安全保護領域間でデータを転送できるようにするための安全な手段を提供することにある。

#### 【0008】

【課題を解決するための手段】本発明により、機密レベル変更カット・アンド・ペースト操作に関するコンパートメント化モード・ワークステーション(CMW)要件の機能を満たすように構成可能な機構が提供される。この機構は、基礎となるオペレーティング・システムが何であってもそのオペレーティング・システムで使うことができる。CMWのカット・アンド・ペースト要件を満たし、機密レベル変更選択機構が抜け道として機能するのを防止するため、本発明の機密レベル変更選択機構の解決策は以下の特徴を有する。

- ・Xサーバは、MAC上位移行操作中の低レベル・プロセスへの通信にダミー・ウィンドウIDを使用する。
- ・すべての機密レベル変更操作について、選択が転送される前にXサーバは、転送の続行を許可する前にユーザ確認を要求するポップアップを表示するよう選択マネージャに指示する事象を選択マネージャに送信する。この選択機構は、カット・アンド・ペースト用の構成可能な機密レベル変更選択操作をサポートする(MAC上位移行はすべてのユーザが対象、MAC下位移行は特権ユー

ザが対象、情報ラベルの上位移行と下位移行はすべてのユーザが対象)。Xウィンドウの選択は仲介された双方向通信を伴うので、それが「抜け道」として使用されるのを防止するため(また、CMWのカット・アンド・ペースト要件を満たすため)に、安全な選択機構によって以下の特徴も提供される。

1. 選択マネージャは、選択項目所有者の安全保護属性を継承する特殊なウィンドウとプロパティを作成し、これを選択項目所有者が使用できるようにする。このため、選択の要求側によって指定されたウィンドウIDとプロパティIDは選択項目所有者から隠される。これは、MAC上位移行時に要求側が低レベル・プロセスと通信するときに選択の所有者が要求側に関する安全保護関連情報を入手できないように行われる。

- 1 a. 選択項目所有者は、通常のX機構により選択マネージャに選択項目データを転送する。選択マネージャは、データの所有者になり、転送が完了するまでそれに対する排他的権利を有する。

2. 選択項目所有者から選択項目要求側に転送されるデータをログイン・ユーザが確認できるようにするユーザ・インタフェースが提供される。これにより、ユーザはいつでも増分転送を取り消すこともでき、機密レベル変更操作の場合にはデータ転送の続行が許可される前にユーザ確認が要求される。

- 2 a. ユーザが転送を確認すると、選択マネージャはデータを要求側に転送する。もう1つのコピーを作成する必要性を回避するため、「所定の場所で」転送を行うために新しいプロトコル要求が使用される。

3. 特権の使用を伴う操作(MAC下位移行など)を試みる場合、ならびにデータ転送、再分類、特権の使用を伴う安全保護違反を犯した場合には、適切な監査事象が生成される。

4. 適切に構成されている場合、選択機構は、要求側のウィンドウおよびプロパティに関する任意アクセス制御(DAC)書込みアクセス制限を無効にするための十分な特権を有する。本発明による機構では、すべてのアプリケーションが機密レベル変更選択バッファに書込みアクセスすることができる。選択バッファに書き込まれるデータは、選択より高レベルにすることができ、それにより、情報ラベルが浮動し、LabelChange事象という新しい事象が生成される。選択項目に書き込むと、書込みプロセスがその選択バッファの「所有者」になり、選択バッファが所有者のラベルを継承する。特定の選択項目の保有者が誰であるかの確認を別のアプリケーションが必要とする場合は、情報を要求したアプリケーションより選択項目の現在の保有者の方が機密レベルが高ければ、何も返されない。これにより、選択項目所有権パターンによって情報の抜け道が間接的に防止される。選択バッファ内のデータをコピーできるかどうかは、保有者のアクセス特権によって決まる。情報を要求したアプリ

ケーションに特権が与えられていない限り、そのアプリケーションより選択バッファの方が機密レベルが高ければ、アプリケーションは選択項目内のデータを読み取ることができない。

【0009】上記およびその他の目的、態様、利点は、添付図面を参照しながら本発明の好ましい実施例に関する以下の詳細な説明を読めば、よりよく理解できるであろう。

#### 【0010】

【発明の実施の形態】Xウィンドウ・システム的环境下で本発明の好ましい実施例について説明するが、本発明は他のウィンドウ環境でも実施可能であることに留意されたい。すべての機密レベル変更カット・アンド・ペースト操作に対し、Xサーバと、選択マネージャという本発明による新しいクライアントを使用する。

【0011】ここで添付図面、特に図1を参照すると、同図には本発明の好ましい実施例による設計済みCMW用の安全なXウィンドウ・システムの構造が示され、新しい承認クライアントの1つとして選択マネージャ100が示されている。より具体的には、通常、Xウィンドウ・システムは、ローカル・エリア・ネットワーク（LAN）などの通信媒体103により接続された複数のXサーバ101および102を含む。それぞれのXサーバには、ユーザがウィンドウ・システムと対話するためのディスプレイ104、キーボード105、マウス106が備えられている。通信媒体103には、本発明による新しい承認クライアント・プログラムである選択マネージャ100を含む、様々なアプリケーションおよび管理プログラムが接続されている。他の管理プログラムとしては、監査マネージャ107、プロセス・マネージャ108、MWMウィンドウ・マネージャ109、XDMディスプレイ・マネージャ110などがある。Xアプリケーション111の他に、擬似端末装置として機能し、接続されたAIXterm端末アダプタ114を介して通信媒体103と通信するマルチレベル・アプリケーション112と通常アプリケーション113が存在する場合もある。Xサーバ101または102は、ユーザが使用しているものと同じワークステーション上で動作しなければならない。クライアントはこのマシン上にある場合もある。他のマシン上にある場合もある。（通常、ウィンドウ・マネージャ109や選択マネージャ100のような「特殊」クライアントは、同一マシン上でローカルに動作するが、これは必須ではない。）

【0012】選択項目はXウィンドウの資源である。選択項目により、アプリケーションは任意のタイプのデータを交換することができ、交換するデータのタイプを折衝することができる。クライアント間通信規則マニュアル（ICCCM）によれば、選択はクライアント間のカット・アンド・ペースト操作に適した方法である。したがって、本発明による解決策では、機密レベル変更カッ

ト・アンド・ペースト操作のベースとして選択資源を使用する。この手法はX選択資源の現在の使い方と整合するものである。というのは、この手法ではX選択資源自体を変更するわけではないが、安全保護レベルの機密レベル変更のためのデータ転送に現在使用されているステップ間に追加ステップを挿入するからである。このため、この解決策は、既存の選択資源の当然の拡張として機能する。

【0013】X選択資源の目的は、複数のアプリケーションが情報を共用できるようにすることである。各選択項目は、一度に1人の「所有者」すなわちトークンの保有者しか持てないため、その所有者はカットまたはペースト操作を実行することができる。1つのアプリケーションがカットを行い、別のアプリケーションがペーストを行う場合は、両方のアプリケーションが先在するX選択要求事象により互いにやりとりする。ワークステーションにとってグローバルな選択項目の数はいくつでもよい。それぞれの選択項目は、アトムによって命名され、クライアントによって所有され、ウィンドウに接続される。

【0014】機密レベル変更選択機構の目的は、適切なMACラベルおよび情報ラベルをペースとするデータに関連づけることである。これは、ポップアップの使用により対話式に、または選択マネージャの構成資源ファイルの構成オプションの設定により非対話式に行うことができる。いずれの場合でも、データのラベル変更に関する標準方針は変わらない。すなわち、MACラベルの上位移行はすべての特権ユーザと通常ユーザに許可され、MACラベルの下位移行は特権ユーザだけに許可され、情報ラベルの上位移行または下位移行はすべての特権ユーザと通常ユーザに許可される。（実際に使用する方針もシステム管理者によって構成可能である。）ユーザがすべてのラベル変更を認識するように、CMWの要件の1つである対話式で機密レベル変更を行う方法について以下に説明する。

【0015】図2は、非増分カット・アンド・ペーストを示している。これは、データ転送が1回だけ行われること、すなわち、すべてのデータが同時に転送されることを意味する。図2のアスタリスク\*は、選択マネージャがXSendEventを使用してこの事象を送信し、他のすべての事象はXサーバによって送信されることを意味する。増分転送では、所与の時点でデータの一部分だけが転送され、1回の転送ごとに所与の検査を行わなければならない。まず図2を参照して非増分ケースについて説明し、次に図3を参照して増分カット・アンド・ペースト操作について説明する。ただし、図2および図3にXサーバが示されていないくても、このプロセスにはXサーバがかかわる（Xサーバによって送信される事象のうち、後ろにアスタリスクが付いていない事象のすべて）ことに留意されたい。また、構成可能なオプションがす

べて設定されているものとして説明を進めることにも留意されたい。たとえば、システム管理者がそのオプションを禁止した場合には、以下に説明するポップアップ・メニューが表示されない場合がある。

【0016】図2は、単純な（非増分）選択に関する選択要求を要求するための修正済みプロトコル内の選択項目要求側と選択項目所有者との間のプロトコルを示している。第1のステップでは、要求側がXConvertSelectionプロトコル要求を出し、それをXサーバがSelectionRequestLabelプロトコル要求に変換し、SelectionRequestLabel事象として選択マネージャに転送する。選択マネージャは、図のステップ2に示すようにMACダイアログとDACダイアログを表示する。ステップ3では、選択マネージャが専用のウィンドウ上でプロパティを作成し、選択項目の所有者は後でそのウィンドウ上でその選択項目をポストすることができる。次に選択マネージャはステップ4でSelectionRequestを生成し、これを最初に意図した受信側に送信する。これは標準のSelectionRequest事象なので、この環境で機能するように受信側のコードを変更する必要はない。

【0017】選択マネージャは、この事象でそれ自体のプロパティを示す。この事象に応答して、選択項目所有者がステップ5で選択マネージャのプロパティで選択項目データをポストし、ステップ6で選択マネージャに対してSelectionNotify事象を出す。次に選択マネージャは、ステップ7で選択項目所有者から選択項目要求側に渡されるデータをユーザが検査できるようにする。これにより、ユーザは、未修正の通過の要求を許可するか、要求を取り消すか、または転送中のデータを下位移行できるようにする。要求を取り消すと、ステップ8で監査事象を生成することができる。この場合、選択マネージャは続行する前に監査レコードが書き出されるのを待つ。これは、ダイアログのステップ9に示されている。ステップ10では、選択マネージャが新しいXTransferProperty呼出しを使用して、それ自体のウィンドウ／プロパティから選択項目要求側のウィンドウ／プロパティに選択項目データを転送する。次に選択マネージャはステップ11でSelectionNotify呼出しを出し、その結果、元のXConvertSelection呼出しに指定されたプロパティでその選択項目が使用可能かどうかを要求側に通知される。ステップ12では、要求側がそのデータを読み取り、次にステップ13でXPropertyNotify呼出しを出し、その結果、選択マネージャに事象が送信される。選択マネージャはステップ14でそれ自体のデータ構造を終結し、ステップ15でプロパティ通知を所有者に転送する。したがって、所有者は、この時点で必要とするすべての終結処置を実行することができる。これで、図2に示すハンドシェークにかかわるすべてのステップの説明を完了する。

【0018】図3は、増分選択項目が転送されていると

きに行われるハンドシェーク・プロトコルを示している。増分選択項目は、1つの選択項目としてではなく、複数の部分に分けて転送することに意味があるほど、大きいものである。このプロトコルは、要求側がまずそれ自体のウィンドウでダミー・プロパティを出すことから始まる。要求側はXConvertSelectionプロトコル要求を出し、それをXサーバがSelectionRequestLabelプロトコル要求に変換し、SelectionRequestLabel事象として選択マネージャに転送する。ステップ2では、非増分ケースのように選択マネージャがMACダイアログとDACダイアログを表示する。ステップ3では、選択マネージャは、選択項目の所有者が後でその選択項目をポストすることができる専用のウィンドウ上でプロパティを作成し、MACダイアログとDACダイアログを表示する。次に選択マネージャは、ステップ4で選択項目所有者に要求を転送する。ステップ5では、選択項目所有者（これが増分選択項目であることを認識している所有者）が選択マネージャのウィンドウ上でそのプロパティをポストし、次にステップ6で、これが増分（INCR）選択項目であることを選択マネージャに通知するSelectionNotifyを出す。したがって、選択マネージャは、そのデータが複数の部分に分かれて到着する（可能性がある）ことを認識する。次に選択マネージャは、ステップ7で選択項目所有者から選択項目要求側に増分式に渡されるデータをユーザが検査できるようにする。要求を取り消すと、ステップ8で監査事象を生成することができる。ステップ9では、選択マネージャが新しいXTransferProperty呼出しを使用して、それ自体のウィンドウ／プロパティから選択項目要求側のウィンドウ／プロパティに選択項目データを転送する。次に選択マネージャは、ステップ10でSelectionNotify（INCR）呼出しを出す。したがって、要求側は、そのデータが複数の部分に分かれて到着する可能性があることを認識する。実際のデータ転送は、ステップ11～14で一連のChangePropertyメッセージとPropertyNotifyメッセージを使って行われる。選択マネージャは、データのレベルを検査して変更し、いつでも選択項目を取り消すことができる機会をユーザに与える。選択マネージャは、1回の転送分としてそれぞれの部分を転送する。唯一の違いは、要求側が個別のXconvertselection要求を送信するのではなく、要求側が転送されたデータを読み取って削除することによって、その後の転送が通知される点である。

【0019】このプロトコルの最後のステップは、ステップ13に示すように、プロパティ所有者が選択マネージャのプロパティで長さがゼロのプロパティ（ダミー）をポストすることである。これにより、転送が完了したことが通知され、それに応答して選択マネージャがステップ14でこの情報を選択項目要求側に転送する。これで選択項目要求側は転送が完了したことと、ステップ1



5～1.7の単一転送ケースのようにハウスキーピング・プロセスを認識することになる。

【0020】このプロセスについては、図4の流れ図に示す。データ転送を行うためには、データ所有者は選択資源所有者にならなければならない。選択アトムは公用資源なので、どのクライアントも選択項目所有権を確認することができる。クライアントがこのデータの受取りを必要とする場合、そのクライアントはデータの所有者にXConvertSelection要求を送る。このXconvertselection要求を受け取ると、Xサーバは、要求を行ったクライアントがその宛先として指定している要求側のウィンドウとプロパティに対して正しいアクセス権を持っていることを確認する。正しいアクセス権を持っている場合には、Xサーバは、SelectionRequestLabel事象という新しい事象としてこのSelectionRequest事象を選択マネージャに転送する。この事象は、選択項目所有者のMAC、ユーザID (UID)、グループID (GID)と、要求側のウィンドウおよびプロパティに関するMACラベルおよびDAC属性とを含んでいる。この事象を受け取る際の選択マネージャの挙動は構成可能である

(すなわち、システム管理者の資源ファイル内の使用に依存する)が、デフォルト挙動では、同じMACレベルの要求がMACアクセス検査に合格する(そして監査を受けない)。

【0021】特に図4を参照すると、まず判断ブロック401では、要求側のMAC (Rmac) が所有者のMAC (Omac) より大きい、等しい、小さいかを判定するためにテストが行われる。要求側が所有者とは異なるMACレベルにある場合、選択マネージャは、判断ブロック402でそのユーザが特権下移行者であるかどうかを確認し、判断ブロック403で上位移行が許可されているかどうかを確認する。いずれの場合にも、選択マネージャはまず、ユーザ・ログイン時にディスプレイ・マネージャ (xdm) によってルート・ウィンドウ・プロパティとしてポストされたユーザおよびグループ・リストを入手する。次に、下移行特権の有無を検査するために、選択マネージャは、それ自体を承認プロセスとして指定し、下移行特権の有無を検査することと、パラメータとしてユーザID (UID) およびグループID (GID) とを指定して、AIXのtc1 (承認プロセス制御リスト) 機能呼出し (他のオペレーティング・システムの場合は、同様の機能を持つシステム呼出し) を行う。(AIXはIBMの商標であり、UNIXオペレーティング・システムのIBM版である。)

【0022】判断ブロック402でユーザが特権下移行者であるかどうかを判定するテストを行うケースを考慮すると、ユーザが特権下移行者ではないと判定された場合、その結果、機能ブロック404に示すように、要求失敗が発生する。すると、図5に示すポップアップが表示され、機能ブロック405で要求側に失敗事象が

送られ、システムへの復帰が行われる前に機能ブロック406で選択マネージャが監査事象を生成する。これに対して、ユーザが特権下移行者である場合は、図6に示すポップアップが表示され、ユーザに下移行確認を要求する。判断ブロック407で判定されたように、ユーザがポップアップから「取消し」を選択した場合は、図5に示すポップアップが表示され、機能ブロック405で要求側に失敗事象が送られ、システムへの復帰が行われる前に機能ブロック406で選択マネージャが監査事象を生成する。ユーザが図6に示すポップアップから「OK」を選択した場合は、機能ブロック408で監査事象が生成される。というのは、下移行はユーザのための許可の用途の1つであるからである。

【0023】判断ブロック403で上位移行が許可されているかどうかを判定するテストを行うケースを考慮すると、上位移行が許可されていないと判定された場合、その結果、図6に示すポップアップが表示される。これは、MAC上位移行警告である。ユーザが「取消し」を選択した場合は、図5に示すポップアップが表示され、機能ブロック409で要求側に失敗事象が送られ、システムへの復帰が行われる前に機能ブロック410で選択マネージャが監査事象を生成する。これに対して、ユーザが図6に示すポップアップで「OK」を選択したか、判断ブロック401で判定されたように要求側ウィンドウMACと所有者プロセスMACが等しい場合には、判断ブロック411で書き込みアクセスが要求されたかどうかを判定するテストが行われる。書き込みアクセスが要求されていない場合は、図7に示すポップアップが表示され、転送を続行すべきかどうか示すようユーザに要求する。判断ブロック412で判定されたように、ユーザが図7のポップアップで「取消し」を選択した場合は、図8に示すポップアップが表示される。次に機能ブロック405で要求側に失敗事象が送られ、システムへの復帰が行われる前に機能ブロック406で選択マネージャが監査事象を生成する。ユーザが図7に示すポップアップで「OK」を選択したか、判断ブロック411で判定されたように書き込みアクセスが要求された場合には、機能ブロック413で所有者がプロパティを書き込む。機能ブロック414では、さらにデータが修正されるのを防止するため、選択マネージャがプロパティの所有権を自分自身に変更する。次に機能ブロック415では、図9に示すポップアップが表示され、要求されたデータに関するラベル情報を提供するように要求側に要求する。

【0024】この時点で、これが増分 (INCR) 転送であるかを判定するテストが判断ブロック416で行われる。増分転送である場合には、次に、これが増分転送の最初の部分であるかどうかを判定するテストが判断ブロック417で行われる。最初の部分である場合には、図10に示すポップアップが表示され、1回のデータ転送ごとに情報ラベルを求めるプロンプトが必要かどうか



を示すよう、要求側に要求する。図10のポップアップから要求側が何を選択しても、図3に関連して記載したプロトコルに従って、機能ブロック418で最初にヘッダが要求側に転送され、機能ブロック419で選択項目データの残りの部分が所有者から増分式に獲得され、プロセスはループをたどって機能ブロック414に戻る。毎回情報ラベルを要求することを要求側が選択した場合には、1回のデータ転送ごとに図11に示すポップアップが表示され、要求側に情報ラベルを要求する。増分転送ではないか、増分転送の最初の部分以降ではない場合には、図12に示すウィンドウが表示され、図2および図3に関連して記載したプロトコルに従って、機能ブロック419でシャドー・ウィンドウから要求側ウィンドウにプロパティが転送される。

【0025】簡単に要約すると、下位移行または上位移行カット・アンド・ペースト操作の許可がユーザに与えられていない場合、選択マネージャは、図5に示す警告ボックスを表示し、拒否を示す監査事象を作成し、プロパティなしを指定したSelectionNotify事象を要求側に返し、選択プロセスを終了する。MAC検査が成功した場合は、選択マネージャはDACアクセス検査を実行する。要求側ウィンドウ／プロパティが所有者に書き込みアクセスを許可していない場合は、図7に示すDACダイアログ・ポップアップにより、そのユーザが要求側のウィンドウまたはプロパティへの書き込みアクセスを所有者プロセスに許諾する必要があるかどうかの質問が行われる。ユーザが肯定の応答を行うと、これは、ウィンドウ／プロパティへの要求側の書き込みアクセスを所有者に与える効果を持ち、特権の使用に関する監査事象（ただし、選択マネージャはDAC免除者である）が生成される。ユーザはMAC問題が一切発生しないときにカット・アンド・ペースト操作の実行が許可されるので、これは、アクセス制御リスト（ACL）とは無関係にペースト操作をサポートするすべてのウィンドウについて許可される。システムがDACを迂回するように構成されていない場合は、図8に示す警告が表示され、選択が失敗に終わり、監査事象が生成される。上記のMAC検査とDAC検査が成功すると、選択マネージャは、カット・アンド・ペースト操作に使用する「シャドー」ウィンドウと「シャドー」プロパティを作成する。この新しいウィンドウとプロパティには、所有者のMACレベルなど、選択項目所有者の安全保護属性が与えられる。これにより、選択項目所有者は選択項目データを安全に書き出せるようになる。（選択マネージャには特権が与えられているので、このウィンドウとプロパティにいつでもアクセスすることができる。）この「シャドー」ウィンドウIDと「シャドー」プロパティIDは、選択項目所有者に送られる後続のすべての事象の際に、要求側のウィンドウIDとプロパティIDの代わりに使用される。このため、要求側のウィンドウIDとプロパティIDが

所有者から隠され、所有者は別のMACレベルにあると思われるウィンドウおよびプロパティのIDを確認できなくなる。その場合、選択マネージャは、データ所有者に送るSelectionRequest事象を作成する際に要求側のIDの代わりにこれらのIDを挿入する。また、選択マネージャは、要求側のウィンドウ上でPropertyNotify事象の送信請求も行うので、データ所有者へのこれらの事象の送信を仲裁し、「シャドー」ウィンドウIDと「シャドー」プロパティIDを挿入することができる。

【0026】所有者がSelectionRequest事象を受け取ると、データ所有者は、XchangeProperty呼出しを使用することにより、「シャドー」プロパティ上にデータをポストする。次に選択項目所有者は、「シャドー」ウィンドウIDと「シャドー」プロパティIDとを使用して、そのデータがプロパティにポストされたことを要求側に示すSelectionNotify事象を要求側に送信する。このSelectionNotify事象はXサーバによって仲裁され、Xサーバはそれに代わって新たに定義されたSelectionLabel事象を選択マネージャに送る。その事象は、要求側クライアントおよび要求側のウィンドウの情報ラベルと、所有者クライアントの情報ラベルとを含む。（これは、選択マネージャによる追加照会の必要性をなくすために行われる。）SelectionLabel事象を受け取ると、選択マネージャはまず、そのデータの所有権を自分自身に変更する。これにより、選択マネージャによる偶発的または作為的なデータの変更が防止される。特に、これにより、黙認している選択項目所有者がユーザ承認のために無害のデータを提示し、承認後（ただし、データが実際に要求側に転送される前）に機密データを密かに挿入することが防止される。選択マネージャは、選択マネージャのシステム管理資源ファイルで選択された構成オプションに応じて、選択項目データの情報ラベルを宛先のウィンドウの情報ラベルあるいは入力情報ラベルまたは要求側クライアントの情報ラベルのいずれかと比較する。情報ラベルを要求するよう構成されている場合、選択マネージャは、図10に示すダイアログ・ボックスを表示し、そのデータの情報ラベルをユーザに要求する。

【0027】上記のように、このダイアログ・ボックスにより、ユーザは選択項目のラベル情報を希望通りに変更することができる。OKを選択した場合は、その選択項目のラベルが変更され（必要な場合）、監査事象が作成される。取消しを選択した場合は、（ICCCM通りに）選択項目が削除され、プロパティなしを指定したSelectionNotify事象が要求側に送られる。取得オプションは、対応する表示ウィンドウ・ラベルを選択項目ラベル（さらに編集される可能性がある）にコピーする。ユーザが無効なラベルを入力すると、エラー・ポップアップのメッセージ域に"Invalid label please re-enter"というメッセージが表示され、監査事象が生成され、ユーザはラベルを再入力する機会を得る。このメッセージ

は、そのデータについて入力された情報ラベルが要求側のプロパティのMACレベルより高い場合にも表示される（この場合にも監査事象が生成される）。ユーザは、そのデータに関する情報ラベルを選択する前にデータを表示する機会も与えられる。（選択マネージャは、テキスト、ビットマップ、ピクセルマップ、整数という「標準」形式をサポートしている。他のタイプのサポートは、タイプ固有のハンドラを組み込むことによって追加することができる。未知のデータ・タイプはいずれも16進ダンプとして表示される。）データを表示する場合、選択マネージャは、プロパティから「シャドー」ウィンドウにデータを移し、それを図12に示すウィンドウに表示する。

【0028】情報ラベル変更サブウィンドウをクリックすると、ユーザは、データを表示している間に対話式に選択項目データにラベルを付けることができる。ユーザに対して情報ラベルが一切要求されない場合（すなわち、情報ラベルの要求を禁止するようにシステム管理者が資源ファイルでそのオプションを構成してある場合）には、情報ラベルが異なっても（すなわち、選択項目データのラベルがデフォルトで選択されても）選択が進行するが、この違いを示す監査事象が生成される。

【0029】監査マネージャは、その初期設定プロセスを完了した後、監査マネージャが監査事象を受け入れられる状態になっていることを選択マネージャ、Xサーバ、その他の特権クライアントに伝えるルート・ウィンドウ・プロパティをポストする。選択マネージャは、このルート・ウィンドウ・プロパティの有無を検査した後、新たに定義したAuditNotify事象を使用して監査マネージャに監査情報を送信する。このAuditNotify事象は、事象が生成された理由（たとえば、特権の使用／誤用、データのラベル変更など）を示すものである。また、この事象は、「シャドー」ウィンドウIDと「シャドー」プロパティIDならびにソース・ウィンドウと宛先ウィンドウのウィンドウIDとプロパティIDも含んでいる。前述の図2および図3のステップ8に示すように通常のカット・アンド・ペースト・プロセス（すなわち、違反なし、特権の使用なし）の一部として選択マネージャによってAuditNotify事象が送られる場合は、監査データをポストする必要がない。カット・アンド・ペーストがMACラベルの下位移行を伴っていた場合（すなわち、ユーザが下位移行者特権を有していた場合）は、CMW要件により、選択項目データも監査レコードに含まれていなければならない。したがって、選択マネージャは「シャドー」ウィンドウIDと「シャドー」プロパティIDを監査事象に含める。監査マネージャはこれらを使用して、データのコピーを入手し、それを監査証跡に入れる。（データが多すぎて1つの監査レコードで処理できない場合は、元のレコードに次のレコードへのリンクを含める。）次に、選択マネージャは、監査マ

ネージャがAuditNotifyタイプを指定したClientMessage事象を送り返して、監査レコードの作成とその監査証跡バッファへの接続を完了したことを選択マネージャに示すまで待つ。

【0030】監査マネージャからClientMessage事象を受け取った後、選択マネージャは、新たに定義したXTransferPropertyというXlibの呼出しを呼び出して、

「シャドー」プロパティから要求側のウィンドウに関連するプロパティにデータ・ポインタを移動する。その結果、このプロパティは要求側からアクセス可能になる。

XTransferProperty呼出しが失敗すると、選択マネージャは、なしというマークを付けたSelectionNotify事象を作成し、これを要求側に送信する。XTransferProperty呼出しからエラーが一切返されない場合は、選択マネージャは、要求側のウィンドウIDとプロパティIDと

を含むSelectionNotify事象を作成し、これを要求側に送信する。ICCCM要件により、要求側はそのプロパティからデータを読み取って、プロパティを削除し、その結果、PropertyNotify事象が送信される。PropertyNotify事象を受け取ると、選択マネージャは「シャドー」ウィンドウと「シャドー」プロパティを削除する。所有者が「シャドー」ウィンドウ上でPropertyNotify事象を送信請求している場合、所有者は、この事象を受け取ると、選択操作が完了したことを認識する。

【0031】増分カット・アンド・ペーストは、所有者が「シャドー」ウィンドウ上にデータをポストする時点まで、上記の非増分カット・アンド・ペーストと同じように進行する。所有者がデータの増分送信を必要とする場合は、所有者は、SelectionNotify事象にINCRタイプと転送のサイズを含める。次にXサーバはこれをSelectionLabel事象に含める。上記の図9に示すように選択マネージャが第1のセグメントの情報ラベルを要求した後、ユーザは、図10に示すポップアップを使用して増分転送のオプションを選択するよう要求される。

【0032】ユーザは、それぞれの転送ごとに情報ラベル・ダイアログ・ボックス（図11）を表示させるか、それ以上の情報ラベル・ポップアップは表示させないかを選択することができる。要求側にSelectionNotify事象を送信する場合、選択マネージャはタイプINCRと選択項目のデータの長さを含める。必要であれば、すべてのデータが送信されるまで増分転送ごとに監査事象と情報ラベル・ポップアップを生成されて、増分転送が進行する。所有者がデータ転送を実行すると、長さゼロを指定した「シャドー」プロパティに関するPropertyNotify事象が送信される（定義により、データを一切含まないオブジェクトにはシステム・ローという情報ラベルが付いているので、転送されたプロパティの長さがゼロの場合、選択マネージャは情報ラベル・ダイアログ・ボックスを一切表示しない）。要求側のプロパティに関して長さゼロを指定したPropertyNotify事象を受け取ると、

選択マネージャは、データの最後の部分が要求側によって削除されたことを認識する。次に選択マネージャは「シャドー」プロパティと「シャドー」ウィンドウを削除する。所有者は、所有者がこの事象を送信請求していると想定した、「シャドー」プロパティに関して長さゼロのPropertyNotify事象を受け取る。これで増分転送が完了する。

【0033】要求側がXConvertSelectionプロセスのターゲットとして複数をリストする場合、要求側は、複数のXConvertSelection要求を送信しなければならないわけではなく、一度に複数のプロパティに選択項目を転送するよう所有者に要求している。これは、要求側と所有者が同じMACレベルにある場合のみ許可されるので、Xサーバが複数の要求について偽IDを生成することはない。上記のものと唯一の変化は、ペースとするデータについて新しい情報ラベルを要求するときに、データが転送されるすべてのプロパティをリストし、そのうちの1つを強調表示したボックスをウィンドウ・マネージャが表示する点である。要求側がボタンを押すと、要求側がそのデータ用の新しい情報レベルを入力できるように、強調表示したプロパティについて図11に示すダイアログ・ボックスが表示される。これは、そのプロパティに関するすべてのデータのラベルが変更されるまで続行される。ただし、複数の要求はすべての同じMACレベルにあるプロパティについてのみ機能し、それぞれのプロパティについてラベルを変更すると監査事象が生成されることに留意されたい。

【0034】1つの好ましい実施例に関して本発明を説明してきたが、当業者であれば、特許請求の範囲の精神および範囲内で修正を加えた本発明が実施可能であることを理解できるであろう。

【0035】まとめとして、本発明の構成に関して以下の事項を開示する。

【0036】(1) 安全なウィンドウ・システム用の機密レベル変更選択機構において、前記ウィンドウ・システム上の個別のウィンドウで動作し、それぞれがそのウィンドウ内にデータを表示する、複数のクライアント・プログラムと、あるクライアント・プログラム・ウィンドウから別のクライアント・プログラム・ウィンドウにデータを転送するためのカット・アンド・ペースト操作用の選択マネージャというクライアントとを含み、前記選択マネージャがコンパートメント化モード・ワークステーション(CMW)要件を満たし、状態の変化をアプリケーションに通知するためにアプリケーションに事象を送信し、前記選択マネージャが転送中のデータの所有権およびその他の安全保護プロパティを操作して、制御式検査可能データ転送の実行を可能にすることを特徴とする、機密レベル変更選択機構。

(2) 必須アクセス管理(MAC)上位移行操作中の低レベル・プロセスへの通信時に、前記ウィンドウ・シ

テムがダミーのウィンドウIDを使用することを特徴とする、上記(1)に記載の機密レベル変更選択機構。

(3) すべての機密レベル変更操作について、選択項目が転送される前に前記ウィンドウ・システムが前記選択マネージャに事象を送信し、その結果、転送続行が許可される前にユーザ確認を要求するポップアップを選択マネージャが表示することを特徴とする、上記(1)に記載の機密レベル変更選択機構。

(4) 安全なウィンドウ・システム内で安全保護属性を有するデータを安全に転送する方法において、データへのアクセスに関する事前定義安全保護レベルを有する要求側からデータ転送に関する要求をウィンドウ・システムが受け取るステップと、要求側によって指定されたウィンドウIDとプロパティIDが選択側所有者から隠されて、要求側が必須アクセス管理(MAC)上位移行時に低レベル・プロセスと通信するときに選択項目の所有者が要求側に関する安全保護関連情報を入手できないようにするために、特殊なウィンドウが選択項目所有者からアクセス可能になる、前記ウィンドウ・システム上で動作する選択マネージャというクライアント・プログラムが、選択項目所有者の安全保護属性を継承する特殊なウィンドウとプロパティを作成するステップとを含むことを特徴とする、安全なデータ転送方法。

(5) 前記選択項目所有者が前記選択マネージャに選択項目データを転送するステップであって、転送が完了するまで前記選択マネージャがデータの所有者になり、それに対する排他的権利を有するステップと、前記選択項目所有者から選択項目要求側に転送されるデータをログイン・ユーザが検査できるようにし、機密レベル変更操作について、データ転送の続行が許可される前にユーザ確認を要求するユーザ・インタフェースを提供するステップとをさらに含むことを特徴とする、上記(4)に記載の安全なデータ転送方法。

(6) MAC下位移行の使用にかかわる操作を試みた場合およびデータ転送および再分類にかかわる安全保護違反を犯した場合に監査事象を生成するステップをさらに含むことを特徴とする、上記(5)に記載の安全なデータ転送方法。

(7) 要求側のウィンドウとプロパティに対する任意アクセス制御(DAC)書込みアクセス制限を指定変更するために十分な特権を有する選択機構を提供するステップをさらに含むことを特徴とする、上記(6)に記載の安全なデータ転送方法。

(8) 選択項目要求側と選択項目所有者との間で安全なウィンドウ・システム内で安全保護属性を有するデータを安全に転送する方法において、前記選択項目要求側がウィンドウ・システムを動作させる選択マネージャというクライアントに転送される要求を出すステップと、前記選択マネージャが必須アクセス管理(MAC)ダイアログと任意アクセス制御(DAC)ダイアログを表示す



るステップと、後で選択項目の所有者が選択項目をポストすることができる専用のウィンドウ上で前記選択マネージャがプロパティを作成し、選択項目要求を生成し、最初に意図した受信側として前記選択項目所有者に前記選択項目要求を送信するステップと、前記選択項目要求に応答して、前記選択項目所有者が前記選択マネージャのプロパティ上で選択項目データをポストし、前記選択マネージャに選択通知事象を出すステップと、ユーザが未修正通過の要求を許可するか、要求を取り消すか、または転送中のデータを下位移行できるように、前記選択項目所有者から前記選択項目要求側に渡されるデータをユーザが検査できるようにするステップと、ユーザが要求を取り消した場合に監査事象を生成するステップと、前記選択マネージャがそれ自体のウィンドウ／プロパティから前記選択項目要求側のウィンドウ／プロパティに選択項目データを転送し、そのプロパティ上の前記選択項目の可用性に関する通知を要求側に出すステップと、前記選択項目要求側がデータを読み取り、前記選択マネージャに通知を出すステップと、前記選択マネージャがデータ転送の完了を所有者に通知するステップとを含むことを特徴とする、安全なデータ転送方法。

(9) 前記選択マネージャによる前記転送ステップが増分式に実行され、それぞれの転送ごとに個別にラベルを付けるかどうかを指定するようユーザに要求するステップをさらに含むことを特徴とする、上記(8)に記載の安全なデータ転送方法。

【図面の簡単な説明】

【図1】本発明の好ましい実施例によるXウィンドウC/MWアーキテクチャを示すブロック図である。

【図2】監査を伴う非増分カット・アンド・ペーストの

プロセスを示すブロック図である。

【図3】監査を伴う増分カット・アンド・ペーストのプロセスを示すブロック図である。

【図4】本発明により実施されるデータ転送プロセスの論理を示す流れ図である。

【図5】コンピュータ画面上に表示されるポップアップMAC拒否警報ボックスの模写図である。

【図6】上位移行／下位移行の確認のためにコンピュータ画面上に表示されるポップアップ・ダイアログ・ボックスの模写図である。

【図7】コンピュータ画面上に表示されるポップアップDACアクセス・チェック・ボックスの模写図である。

【図8】コンピュータ画面上に表示されるポップアップDAC拒否警報ボックスの模写図である。

【図9】コンピュータ画面上に表示されるポップアップ・ラベル・ダイアログ・ボックスの模写図である。

【図10】コンピュータ画面上に表示されるポップアップ増分転送メニューの模写図である。

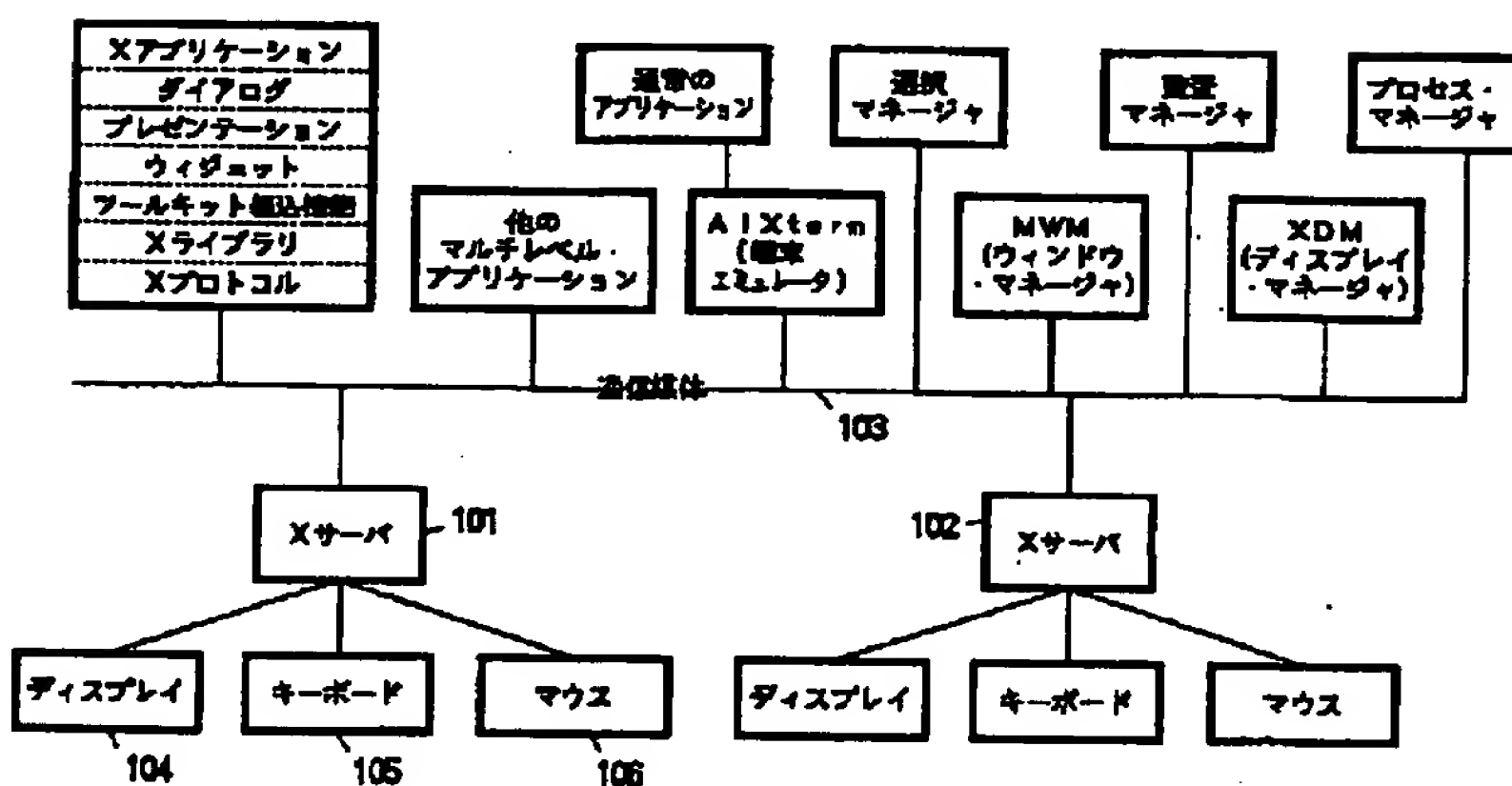
【図11】コンピュータ画面上に表示されるポップアップ選択項目データ・ラベル・ダイアログ・ボックスの模写図である。

【図12】コンピュータ画面上に選択項目データを表示するためのウィンドウ外観の模写図である。

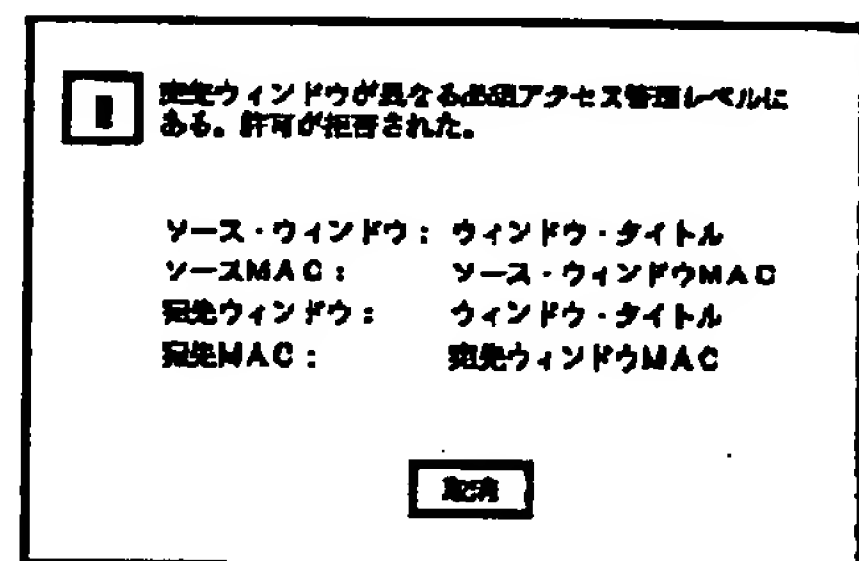
【符号の説明】

- 101 Xサーバ
- 102 Xサーバ
- 103 通信媒体
- 104 ディスプレイ
- 105 キーボード
- 106 マウス

【図1】

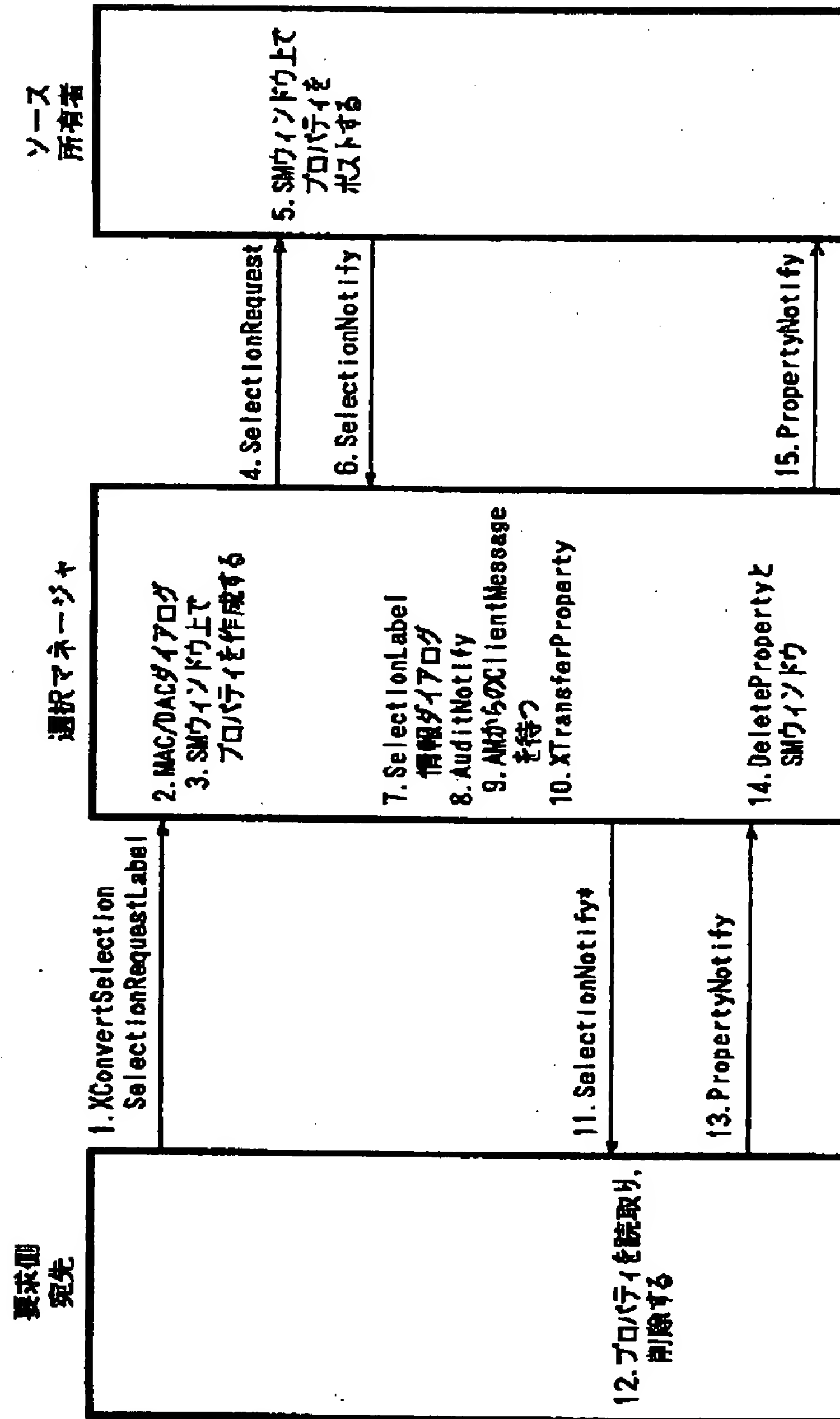


【図5】

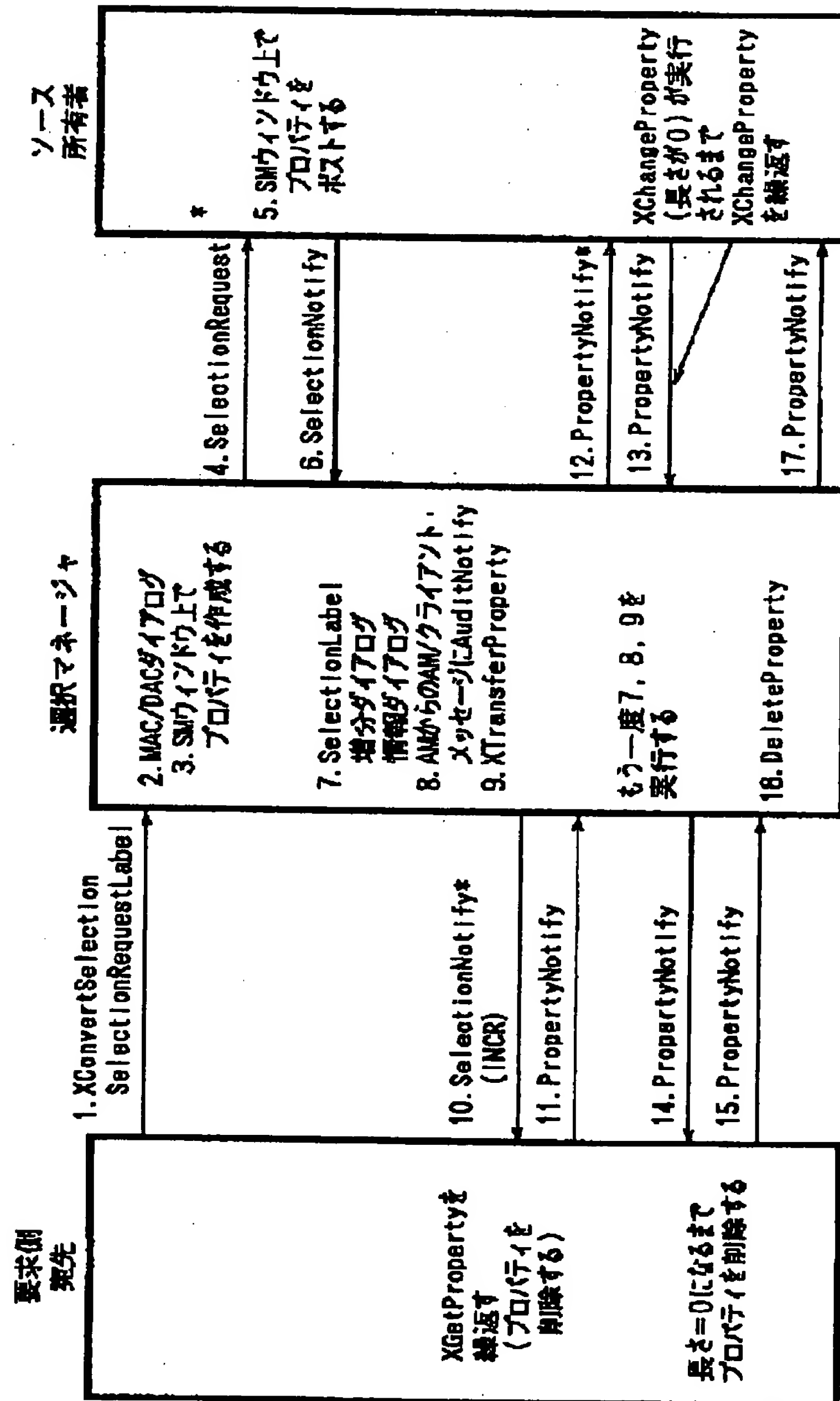




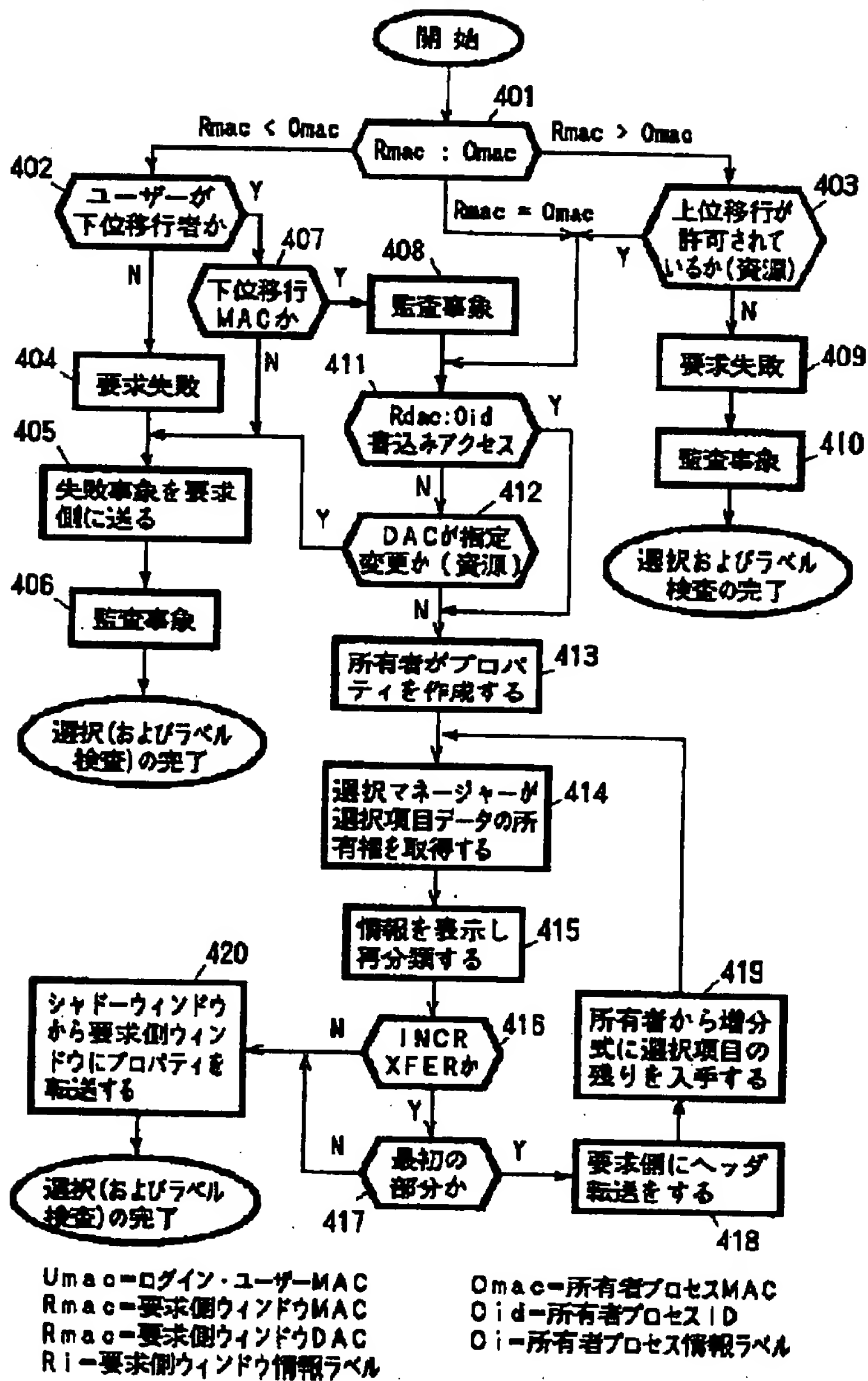
【図2】



【図3】



【図4】



【図7】

データの所有者は要求側のウィンドウまたはプロパティに  
対する書き込みアクセスを持っていない。  
それでも実行するか?

OK 取消

【図6】

？ 実行ウィンドウが異なる必須アクセス管理レベルに  
ある。選択項目転送を続行すべきか？

ソース・ウィンドウ: ウィンドウ・タイトル  
 ソースMAC: ソース・ウィンドウMAC  
 宛先ウィンドウ: 宛先ウィンドウMAC  
 宛先MAC: 宛先ウィンドウMAC

OK 取消

【図8】

！ データの所有者は実行ウィンドウに対する書き込みア  
クセスを持っていない。  
許可が拒否された。

ソース・ウィンドウ: ウィンドウ・タイトル  
 ソース所有者: ソース所有者名  
 宛先ウィンドウ: ウィンドウ・タイトル  
 宛先所有者: 宛先所有者名

取消

【図9】

？ 選択項目にどのようにラベルを付けるか？

宛先ウィンドウ: ウィンドウ・タイトル  
 ウィンドウ・ラベル: ウィンドウ情報ラベル  
 ウィンドウスカラベル: ウィンドウ入力情報ラベル  
 クライアント情報ラベル: クライアント情報ラベル  
 選択項目ラベル: 実行選択項目ラベル(無常可記)

OK データ表示 取消

【図10】

要求されたデータを増分転送中

選択項目ラベル: 実行選択項目ラベル

各情報ラベルを  
要求する 同一情報ラベル追加の  
ポップアップなし

OK 取消

【図11】

?

以下の選択項目にどのようにラベルを付けるか？

宛先ウィンドウ:

ウィンドウ名

ウィンドウ・ラベル:

ウィンドウ情報ラベル

取得

ウィンドウ入力ラベル:

ウィンドウ入力情報ラベル

取得

プロパティ名 1

↑

プロパティ名 2

↑

プロパティ名 3

↑

選択項目ラベル:

選択項目ラベル(編集可能)

OK

取消

【図12】

選択項目名	プロパティ・データ・タイプ
情報レベル変更	取消
選択項目データ	

フロントページの続き

(72)発明者   ムドゥムバイ・ランガナタン  
              アメリカ合衆国20905   メリーランド州シ  
              ルバー・スプリング   スタートヴァント・  
              ストリート   14405

(72)発明者   ジャネット・アン・クジーニ  
              アメリカ合衆国21793   メリーランド州ウ  
              オーカーズヴィル   グレーブ・クリーク・  
              ロード   8998



⑬ 日本国特許庁(JP)

⑭ 特許出願公開

⑯ 公開特許公報(A)

平3-35351

⑮ Int. Cl.<sup>5</sup>

G 06 F 15/20

識別記号

5 9 0 Z  
5 8 6 J

庁内整理番号

7165-5B  
7165-5B

⑯ 公開 平成3年(1991)2月15日

審査請求 未請求 請求項の数 1 (全5頁)

⑰ 発明の名称 文書処理システム

⑱ 特 願 平1-169560

⑲ 出 願 平1(1989)6月30日

⑳ 発 明 者 今 村 泰 介 東京都府中市東芝町1番地 株式会社東芝府中工場内  
 ㉑ 出 願 人 株 式 会 社 東 芝 神奈川県川崎市幸区堀川町72番地  
 ㉒ 代 理 人 弁 理 士 鈴 江 武 彦 外3名

## 明 細 書

## 1. 発明の名称

文 書 処 理 シ ス テ ム

## 2. 特許請求の範囲

承認印イメージが登録される承認印イメージデータベースと、

この承認印イメージデータベースに登録する承認印イメージを第1の条件による保護のもとで作成する承認印イメージ作成手段と、

上記承認印イメージデータベースに登録されている承認印イメージのみが配置可能な文書構造内の承認印用領域を定義する承認印用領域定義手段と、

この承認印用領域定義手段によって定義された上記文書構造内の承認印用領域に、上記承認印イメージデータベースに登録されている承認印イメージを第2の条件による保護のもとで配置する承認印捺印手段と、

上記承認印イメージデータベースに登録されている承認印イメージ以外のイメージが画面上で

上記承認印用領域に表示されるのを抑止すると共に、上記承認印イメージを対象とするコピー操作を抑止する第1の承認印保護手段と、

上記承認印用領域が定義された文書の印刷出力に際し、上記承認印イメージデータベースに登録されている承認印イメージ以外のイメージが上記承認印用領域内に印刷されることを抑止する第2の承認印保護手段と、

を具備することを特徴とする文書処理システム。

## 3. 発明の詳細な説明

## 〔発明の目的〕

(産業上の利用分野)

この発明は、承認印の捺印を電子的に行う文書処理システムに関する。

(従来の技術)

文書の承認行為の一形態として、承認印の捺印が知られている。この捺印行為は、文書(文書本体)をワードプロセッサなどの文書処理システムで作成するようになっても、手作業で行われるのが一般的であった。そこで、承認印の捺印も文

書処理システムにおいて電子的に行えることが要求されている。

さて、文書処理システムにおいて承認印を電子的に捺印する機能を実現しようとする、次の①、②の要素を持つ方式が考えられる。

①承認印はイメージとして作成してデータベースに登録し、そのイメージの作成、変更、登録、削除といった作業に対してはパスワード等の手段を用いて或る特定の限られた人のみが行えるようにする。

②文書内に承認印を押すときには、上記①で作成登録しておいた承認印イメージを用いて文書内の承認印欄に貼り込む。但し、①において各々の承認印イメージ毎にパスワードを付加し、そのパスワードが割当てられた特定の個人以外は該当する承認印イメージが使用できないようにする。

ところで、近年の文書処理システムでは、イメージのコピー等を画面上で簡単に行うことができるようになってきている。また、高密度のイメージスキャナを用いて印刷物から所望のイメージを文

(承認印が電子的に捺印された画面上の文書または印刷文書)から承認印イメージをコピーしたり、偽の承認印イメージを作成して、画面上で文書内の承認印欄に偽の承認印を捺印することができるという問題があった。

この発明は上記事情に鑑みてなされたものでその目的は、承認印を用いた文書の承認行為の電子化が図れ、しかも偽の承認印イメージを作成したり、承認印が電子的に捺印された印刷文書からイメージスキャナによって承認印イメージを切り出したとしても、この種の承認印イメージを用いて電子的な捺印を行うことが確実に防止できる文書処理システムを提供することにある。

#### [発明の構成]

##### (課題を解決するための手段)

この発明は、承認印イメージが登録される承認印イメージデータベースと、この承認印イメージデータベースに登録する承認印イメージを第1の条件による保護のもとで作成する承認印イメージ作成手段と、上記承認印イメージデータベ

(2)

書処理システム内に読み込み、画面上で切り貼りすることも可能である。したがって上記の方式では、承認印イメージが貼り込まれた(即ち承認印が電子的に捺印された)画面上の文書から承認印イメージを切り出してコピーしたり、承認印が電子的に捺印された印刷文書から承認印のイメージをイメージスキャナによって文書処理システムに読み込み、画面上で必要イメージを切り出した後に文書内の承認印欄に貼り込むことが不特定多数の人によって行われる虞がある。

##### (発明が解決しようとする課題)

上記したように従来は、承認印を用いた文書の承認行為を文書処理システムで実現するために、この承認行為に必要な承認印イメージの作成と作成した承認印イメージを用いた文書内の承認印欄への貼り込みを、パスワードを用いて特定の個人だけが行えるようにしても、文書処理システムが持つコピー機能、イメージ作成機能、イメージ入力機能および入力イメージを切り貼りする機能を利用することにより、不特定多数の人が他の文書

に登録されている承認印イメージのみが配置可能な文書構造内の承認印用領域を定義する承認印用領域定義手段と、上記文書構造内の承認印用領域に、承認印イメージデータベースに登録されている承認印イメージを第2の条件による保護のもとで配置する承認印捺印手段と、上記承認印イメージ以外のイメージが画面上で上記承認印用領域に表示されるのを抑止すると共に、承認印イメージを対象とするコピー操作を抑止する第1の承認印保護手段と、文書の印刷出力に際し、上記承認印イメージ以外のイメージが承認印用領域内に印刷されることを抑止する第2の承認印保護手段とを設けたことを特徴とするものである。

##### (作用)

上記の構成によれば、承認印用領域には、承認印イメージデータベースに登録されている承認印イメージだけしか配置できず、しかも承認印イメージの配置は第2の条件(例えば同一イメージに付されるパスワード)の保護のもとで行われる。即ち上記の構成によれば、承認印イメージデータ

(3)

## (実施例)

ベース内の承認印イメージを用いて承認印用領域に承認印を電子的に捺印する操作は、上記第2の条件を満たす人(特別の権限を有する人)に限られ、また第3者が偽の承認印イメージを作成しても、第1の条件(例えばパスワード)を満たさない限りは承認印イメージデータベースに登録されず、したがって正当な承認印イメージとしての扱いを受けないため、このような偽の承認印イメージが承認印用領域に配置される虞はない。このことは、印刷文書からイメージスキャナによって承認印用領域のイメージを読み取り、そこから承認印イメージを切り出して利用しようとする場合にも同様である。また、承認印用領域が定義された文書と偽の承認印イメージを画面表示時または印刷出力時に合成しようとしても、偽の承認印イメージが承認印用領域内に表示または印刷されることが第1の承認印保護手段または第2の承認印保護手段によって抑止されるため、この点からも第3者による承認印の捺印が行われる虞はない。

第1図はこの発明の一実施例に係る文書処理システムのブロック構成を示す。同図において、11は承認印イメージが登録される承認印イメージデータベース、12は承認印イメージデータベース11に登録する承認印イメージ(承認印イメージオブジェクト)を第1のパスワードP1の保護のもとで第2のパスワードP2を付して作成する承認印イメージ作成ツールである。承認印イメージ作成ツール12は、承認印イメージの作成の他に、パスワードP1の保護のもとで承認印イメージデータベース11への承認印イメージ登録、登録した承認印イメージの変更並びに削除の機能を持つ。13は各種文書が格納される文書ファイル、14は文書の作成・編集機能を有する文書編集ツール、15は文書編集ツール14によって作成・編集される文書等の表示に供される表示モニタ、16は図示せぬプリンタ機構を用いて文書等の印刷を行う印刷ツールである。

文書編集ツール14は、承認印イメージデータ

ベース11に登録されている承認印イメージのみが配置可能な文書構造内の承認印用領域(承認印欄)17をパスワードP1の保護のもとで定義する承認印用領域定義機構21と、承認印用領域定義機構21によって定義された文書構造内の承認印用領域17に、承認印イメージデータベース11に登録されている承認印イメージを同イメージに付されているパスワードP2の保護のもとで配置する承認印捺印機構22とを有している。承認印用領域定義機構21は、承認印用領域17の定義(設定、作成)の他に、変更、削除の機能を持つ。文書編集ツール14は更に、各種イメージのコピーおよびペースト(貼り込み)を行うためのコピー&ペースト機構23と、文書等を表示モニタ15に表示するための管理を行う文書表示管理機構24と、コピー&ペースト機構23による承認印イメージのコピーを抑止(禁止)すると共に、正当な承認印イメージ(承認印イメージデータベース11に登録されている承認印イメージ)以外のイメージ(印刷文書等からイメージスキャナを用いて読み込んだ承認印イメ

ージや、特別の権限を持たない人が作成した承認印イメージデータベース11に登録不可能な偽の承認印イメージ等)が文書表示管理機構24によって承認印用領域17内に表示されることを抑止(禁止)する承認印保護機構25とを有している。また印刷ツール16は、正当な承認印イメージ以外のイメージが承認印用領域17内に印刷されることを抑止(禁止)する承認印保護機構26を有している。

次に、第1図の構成の動作を第2図の流れ図を参照して説明する。

まず承認印イメージ作成ツール12は、ユーザからの指示に応じ、パスワードP1の保護(パスワードP1を用いたチェック)のもとで指示された承認印イメージ(承認印イメージオブジェクト)を作成し、第2図において符号1で示されるように、承認印名、承認印イメージ、およびユーザ指定のパスワード(或はユーザに予め割り当てられたパスワード)P2の対から成る承認印イメージ情報(承認印イメージデータ)を承認印イメージデータベース11に登録する(ステップS1)。ここで、パスワードP1を知

らないユーザからの指示は承認印イメージ作成ツール12において排除され、上記の承認印イメージ作成・登録は行われない。

次に文書編集ツール14の承認印用領域定義機構21が起動されると、この承認印用領域定義機構21はユーザからの指示に応じ、パスワードP1の保護のもとで文書ファイル13に格納されている指定文書の文書構造内に承認印用領域17を定義(設定)する(ステップS2)。やがて文書編集ツール14内の承認印捺印機構22が起動されると、この承認印捺印機構22はユーザから指示された承認印イメージをパスワードP2の保護のもとで承認印イメージデータベース11から取り出し、この取り出した承認印イメージを、文書ファイル13に格納されている指定された文書上の承認印用領域17(承認印用領域定義機構21によって定義された承認印用領域17)に配置する(ステップS3)。これにより、承認印の捺印が電子的に行われたことになる。ここで、パスワードP2を知らないユーザからの指示は承認印捺印機構22において排除さ

は入力したイメージ(偽の承認印イメージ)を合成して表示することは不可能である。ここでは、表示対象文書のうちの承認印イメージを除いた部分がまず表示され、次に承認印用領域17が例えば白く塗りつぶされ、この状態で承認印イメージが承認印用領域17に表示される。承認印イメージが承認印用領域17に表示されているときに、コピー&ペースト機構23が起動され、承認印用領域17内のイメージのコピー或はペーストが指示されることがある。しかし本実施例では、承認印用領域17内のイメージを対象とするコピー&ペースト機構23のコピー或はペースト処理は、承認印保護機構25によって抑止される。これは、承認印イメージデータベース11内の承認印イメージについても同様である。

最後に印刷ツール16が起動されると、この印刷ツール16はユーザによって指定された文書を文書ファイル13から取り出し、用紙に印刷出力する(ステップS4)。この結果、承認印用領域17が定義され、同領域17に承認印イメージが配置され

(4)れ、上記の承認印捺印は行われない。また承認印捺印機構22においては、特別の権限を持たない人が作成した承認印イメージデータベース11に登録不可能な偽の承認印イメージ、更には印刷文書の承認印用領域17からイメージスキャナを用いて読み込まれて切り出された承認印イメージをユーザ指定の文書の承認印用領域17に配置することも抑止される。また、承認印イメージデータベース11に格納されている正当な承認印イメージを承認印用領域17以外に配置することも抑止される。

さて、ステップS2において承認印用領域定義機構21によって承認印用領域17が定義された文書、更にはステップS3において承認印捺印機構22によって承認印用領域17に承認印が捺印された文書は、その都度文書表示管理機構24によって表示モニタ15に表示される。この文書表示では、承認印用領域17に関しては承認印保護機構26によって特殊に扱われ、同領域17には承認印イメージだけが表示されるように制御される。したがって、文書の承認印用領域17上に第三者が任意に生成或

ている文書であれば、承認印が捺印された文書が印刷出力されることになる。上記の印刷においては、印刷ツール16内の承認印保護機構26の動作により、文書の承認印用領域17上に第三者が任意に生成或は入力したイメージ(偽の承認印イメージ)を合成して印刷することが抑止される。

#### [発明の効果]

以上詳述したようにこの発明によれば、承認印の捺印対象となる文書構造内に承認印用領域という特別の領域を設定し、この領域にはパスワード等の保護のもとで作成された承認印イメージだけがパスワード等の保護のもとで配置でき、更にこの領域に他のイメージを重ねて表示或は印刷することが抑止される構成としたので、承認印を用いた文書の承認行為の電子化において、偽の承認印イメージを作成したり、承認印が電子的に捺印された印刷文書からイメージスキャナによって承認印イメージを切り出したとしても、この種の承認印イメージを用いて電子的な捺印を行うことを確実に防止することができる。

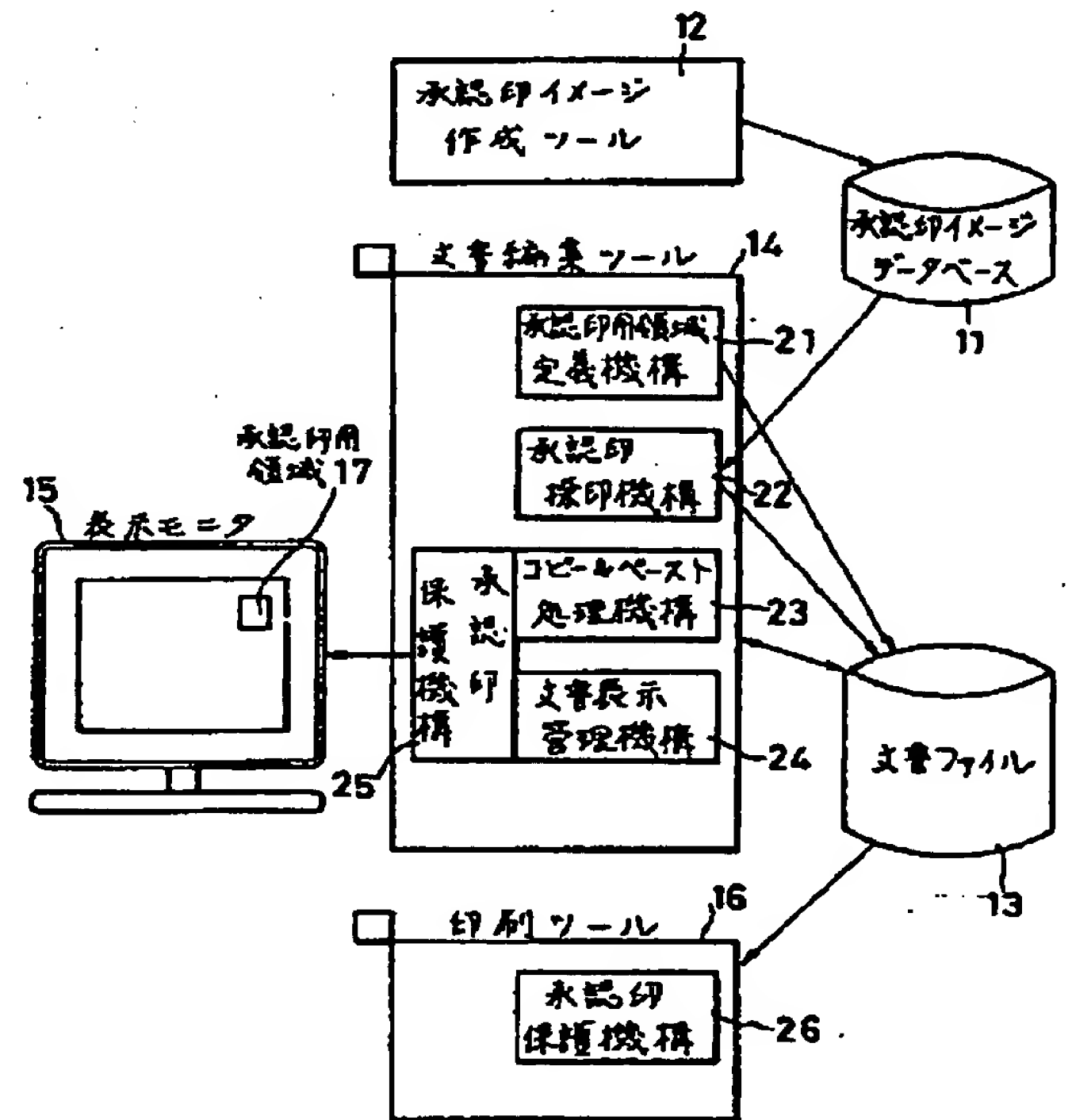


(5)

#### 4. 図面の簡単な説明

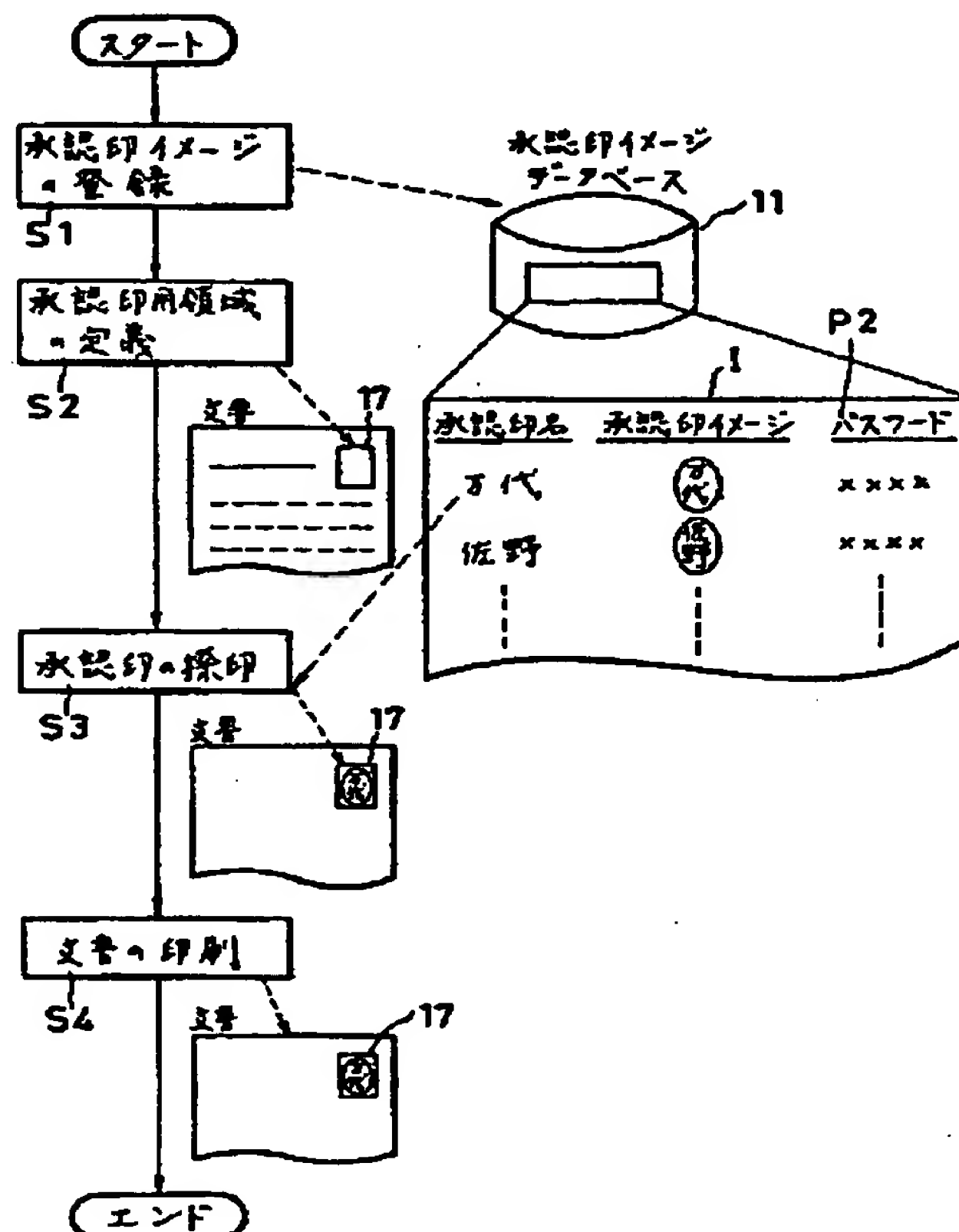
第1図はこの発明の一実施例に係る文書処理システムのブロック構成図、第2図は同実施例における承認印イメージ作成から承認印が捺印された文書の印刷までの動作を説明するための流れ図である。

11…承認印イメージデータベース、12…承認印イメージ作成ツール、13…文書ファイル、14…文書編集ツール、15…表示モニタ、16…印刷ツール、17…承認印用領域、21…承認印用領域定義機構、22…承認印捺印機構、23…コピー&ペースト機構、24…文書表示管理機構、25、26…承認印保護機構。



出願人代理人 弁理士 鈴江武彦

第1図



第2図

## 拒絶理由通知書

特許出願の番号	平成 9年 特許願 第154046号
起案日	平成15年12月22日
特許庁審査官	奥村 元宏 3044 5N00
特許出願人代理人	河野 登夫 様
適用条文	第29条第2項、第36条

この出願は、次の理由によって拒絶をすべきものである。これについて意見があれば、この通知書の発送の日から60日以内に意見書を提出して下さい。

## 理 由

## 理由 1

この出願は、特許請求の範囲の記載が下記の点で、特許法第36条第6項第2号に規定する要件を満たしていない。

## 記

1.

請求項：1－16

備考：

請求項1の「データ」及び「入力データ」という事項は明確でない。特に、これらの事項のみでは、これらのデータを区別できない上に、これらのデータがどのようなデータであり、本願発明が何を行うシステムであるのか、把握することができない。

## 理由 2

この出願の下記の請求項に係る発明は、その出願前日本国内又は外国において頒布された下記の刊行物に記載された発明に基いて、その出願前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから、特許法第29条第2項の規定により特許を受けることができない。

## 記 (引用文献等については引用文献等一覧参照)

請求項: 1-16

引用文献: 1

備考:

引用文献1には、単位著作物を構成する素材データ、被引用作品の作品情報または他の作品中の素材データを特定する引用データ、素材データや引用データに基づいて作品を構成するための指示を与える作品構成データ、及び、作品に付随する知的財産権の権利者、対価額、利用制限を示すデータから構成される財産権データといった各種データによって構成される作品情報を編集・保存する発明が記載されている。

引用文献1に記載された発明において、知的財産として保護される引用データが作品情報に直接格納されることなく、被引用作品の作品情報または他の作品中の素材データを特定するためのデータのみが作品情報に格納されていることは明らかである。また、被引用作品を引用する際に適宜課金が行われることも明らかである。

また、アクセス許可のないデータのカット&ペーストを防ぐ技術は周知のものである。

## 引用文献等一覧

## 1. 特開平7-302244号公報

拒絶の理由が新たに発見された場合には拒絶の理由が通知される。

-----  
先行技術文献調査結果の記録

- ・調査した分野 IPC第7版 G06F12/14
- ・先行技術文献 特開平8-185448号公報 ✓  
特開平8-292976号公報  
特開平8-329011号公報  
特開平8-255132号公報  
特開平3-35351号公報

この先行技術文献調査結果の記録は、拒絶理由を構成するものではない。

この拒絶理由通知についての問い合わせがあるとき、又は、この出願について面接を希望されるときは、以下までご連絡下さい。

連絡先 特許審査第四部情報処理（記憶管理） 高橋 克  
（電話） 03-3581-1101 （内線） 3585